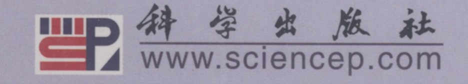
数学机械化丛书

消去法及其应用

王东明 著



数学机械化丛书

消去法及其应用

王 东 明 著

科 学 出 版 社

2002

内 容 简 介

本书系统介绍多项式系统零点分解的消去算法. 这些算法能将任意多元多项式系统分解为三角系统、正则系统、简单系统、具有投影特性的三角系统和不可约三角系统. 各种三角型系统理论上性质殊异, 计算上难易匪同, 应用上则各有所长. 书中还简述基于结式和格罗布讷基的消去算法, 讨论代数簇的等维与不可约分解以及多项式理想的准素分解, 并介绍符号消去法的若干应用, 包括代数方程求解、几何定理求证、多项式因子分解和微分系统的定性分析.

本书可供有关科研和工程技术人员参考, 也可作为高等院校数学和计算机科学系高年级学生及研究生的教学参考书.

图书在版编目(CIP)数据

消去法及其应用/王东明著. —北京:科学出版社,2002.8
(数学机械化丛书/吴文俊主编)
ISBN 7-03-010560-5

Ⅰ. 消… Ⅱ. 王… Ⅲ. 消去法 Ⅳ. O241.6

中国版本图书馆 CIP 数据核字(2002)第 050262 号

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
源海印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2002年8月第 一 版 开本:B5(720×1000)
2002年8月第一次印刷 印张:20 1/4
印数:1—2 000 字数:350 000

定价: 48.00 元

(如有印装质量问题,我社负责调换〈新欣〉)

《数学机械化丛书》获国家基础研究发展规划项目“数学机械化与自动推理平台”与数学机械化应用推广专项经费资助

《数学机械化丛书》前言①

十六七世纪以来，人类历史上经历了一场史无前例的技术革命，出现了各种类型的机器，取代各种形式的体力劳动，使人类进入一个新时代. 几百年后的今天，电子计算机已可开始有条件地代替一部分特定的脑力劳动，因而人类已面临另一场更宏伟的技术革命，处在又一个新时代的前夕. 数学是一种典型的脑力劳动，它在这一场新的技术革命中，无疑地将扮演一个重要的角色. 为了了解数学在当前这场革命中所扮演的角色，就应对机器的作用，以及作为数学的脑力劳动的方式，进行一定的分析.

1. 什么是数学的机械化

不论是机器代替体力劳动，或是计算机代替某种脑力劳动，其所以成为可能，关键在于所需代替的劳动已经“机械化”，也就是说已实现了刻板化或规格化. 正因为割麦、刈草、纺纱织布的动作已经是机械化刻板化了的，因而可据此造出割麦机、刈草机、纺纱机织布机来. 也正因为加减乘除开方等运算这一类脑力劳动，几千年来就已经是机械地刻板地进行的，才有可能使得 17 世纪的法国数学家巴斯喀，利用齿轮传动造出了第一台机械计算机 —— 加法机，并由莱布尼茨改进成为也能进行乘法的机器. 数学问题的机械化，就要求在运算或证明过程中，每前进一步之后，都有一个确定的、必须选择的下一步，这样沿着一条有规律的、刻板的道路，一直达到结论.

在中小学数学的范围里，就有着不少已经机械化了的课题. 除了四则、开方等运算外，解线性联立方程组就是一个很好的例子. 在中学用的数学课本中，往往介绍解线性方程组的各种“消去法”，其求解过程是一个按一定程序进行的计算过程，也就是一种机械的、刻板的过程. 根据这一过程编成程序，由电子计算机付诸实施，就可以不仅机器化而且达到自动化，在几分钟甚至几秒钟之内求出一个未知数多至上百个的线性方程组的解答来，这在手工计算几乎是不可能的. 如果用手工计算，即使是解只有三四个未知数的方程组，也

---

① 上世纪七八十年代之交，我尝试用计算机证明几何定理取得成功，由此并提出了数学机械化的设想. 先后在一些通俗报告与写作中，解释数学机械化的意义与前景，例如 1978 年发表于《自然辩证法通讯》的“数学机械化问题”以及 1980 年发表于《百科知识》的“数学的机械化”. 二文都重载于 1995 年由山东教育出版社出版的《吴文俊论数学机械化》一书. 经过 20 多年众多学者的努力，数学机械化在各个方面都取得了丰富多彩的成就，并已出版了多种专著，汇集成现在的数学机械化丛书. 现据 1980 年的《百科知识》的“数学的机械化”一文，稍加修改并作增补，以代丛书前言.

将是繁琐而令人厌烦的. 现代化的国防、经济建设中, 大量出现的例如网络一类的问题, 往往可归结为求解很多未知数的线性方程组. 这使得已经机械化了的线性方程解法在四个现代化中起着一种重要作用.

即使是不专门研究数学的人们, 也大都知道, 数学的脑力劳动有两种主要形式: 数值计算与定理证明 (或许还应包括公式推导, 但这终究是次要的). 著名的数理逻辑学家美国洛克菲勒大学教授王浩先生在一篇《向机械化数学前进》的有名文章中, 曾列举了这两种数学脑力劳动的若干不同之点. 我们可以简略而概括地把它们对比一下:

计　算	证　明
易	难
繁	简
刻板	灵活
枯燥	美妙

计算, 如已经提到过的加减乘除开方与解线性方程组, 其所以虽繁而易, 根本原因正在于它已经机械化. 而证明的巧而难, 是大家都深有体会的, 其根本原因也正在于它并没有机械化. 例如, 我们在中学初等几何定理的证明中, 就经常要依靠诸如直观、洞察、经验, 以及其他一些模糊不清的原则, 去寻找捷径.

2. 从证明的机械化到机器证明

一个值得提出的问题是: 定理的证明是不是也能像计算那样机械化, 因而把巧而难的证明, 化为计算那样虽繁而易的劳动呢? 事实上, 这一证明机械化的设想, 并不始自今日, 它早就为 17 世纪时的大哲学家、大思想家和大数学家笛卡儿和莱布尼茨所具有. 只是直到 19 世纪末, 希尔伯特 (德国数学家, 1862~1943) 等创立并发展了数理逻辑以来, 这一设想才有了明确的数学形式. 又由于 20 世纪 40 年代电子计算机的出现, 才使这一设想的实现有了现实可能性.

从上世纪二三十年代以来, 数理逻辑学家们对于定理证明机械化的可能性, 进行了大量的理论探讨, 他们的结果大都是否定的. 例如哥德尔 (Gödel) 等的一条著名定理就说, 即使看来最简单的初等数论这一范围, 它的定理证明的机械化也是不可能的. 另一方面, 1950 年波兰数学家塔斯基 (Tarski) 则证明了初等几何 (以及初等代数) 这一范围的定理证明, 却是可以机械化的. 只是塔斯基的结果近于例外, 在初等几何及初等代数以外的大量结果都是反面的, 即机械化是不可能的. 1956 年以来美国开始了利用电子计算机做证明定理的尝试. 1959 年王浩先生设计了一个机械化方法, 用计算机证明了罗素等

著的《数学原理》这一经典著作中的几百条定理，只用了 9 分钟，在数学与数理逻辑学界引起了轰动. 有一时机器证明的前景似乎非常乐观. 例如 1958 年时就有人曾经预测：在 10 年之内计算机将发现并证明一个重要的数学新定理. 还有人认为，如果这样，则不仅许多著名哲学家与数学家，如庞阿诺、怀特海、罗素、希尔伯特以及杜灵等人的梦想得以实现，而且计算将成为科学的皇后，人类的主人！

然而，事情的发展却并不如预期那样美好. 尽管在 1976 年时，美国的哈肯等人，在高速计算机上用了 1200 小时的计算时间，解决了数学家们 100 多年来所未能解决的一个著名难题 —— 四色问题，因此而轰动一时，但是，这只能说明计算机作为定理证明的辅助工具有着巨大潜力，还不能认为这样的证明就是一种真正的机器证明. 用王浩先生的说法，哈肯等关于四色定理的证明是一种使用计算机的特例机证，它只适用于四色这一特殊的定理，这与所谓基础机器证明之能适用于一类定理者有别. 后者才真正体现了机械化定理证明，进而实现机器证明的实质. 另一面，在真正的机械化证明方面，虽然塔斯基在理论上早已证明了初等几何的定理证明是能机械化的，还提出了据以造判定机也即是证明机的设想，但实际上他的机械化方法非常繁，繁到不可收拾，因而远远不是切实可行的. 1976 年时，美国做了许多在计算机上证明定理的实验，在塔斯基的初等几何范围内，用计算机所能证明的只是一些近于同义反复的“儿戏式”的“定理”. 因此，有些专家曾经发出过这样悲观的论调：如果专依靠机器，则再过 100 年也未必能证明出多少有意义的新定理来.

3. 一条切实可行的道路

1976 年冬，我们开始了定理证明机械化的研究. 1977 年春取得了初步成果，证明初等几何主要一类定理的证明可以机械化. 在理论上说来，我们的结果已包括在塔斯基的定理之中. 但与塔斯基的结果不同，我们的机械化方法是切实可行的，即使用手算，依据机械化的方法逐步进行，虽然繁复，也可以证明一些艰深的定理.

我们的方法主要分两步，第一步是引进坐标，然后把需证定理中的假设与终结部分都用坐标间的代数关系来表示. 我们所考虑的定理局限于这些代数关系都是多项式等式关系的范围，例如平行、垂直、相交、距离等关系都是如此. 这一步可以叫做几何的代数化. 第二步是通过代表假设的多项式关系把终结多项式中的坐标逐个消去，如果消去的结果为零，即表明定理正确，否则再作进一步检查. 这一步完全是代数的，即用多项式的消元法来验证.

上述两步都可以机械与刻板地进行. 根据我们的机械化方法编成程序，以

在计算机上实现机器证明，并无实质上的困难．事实上数学所某些同志以及国外的王浩先生都曾在计算机上试行过．我们自己也曾在国产的长城 203 台式机上证明了像西摩松线那样不算简单的定理． 1978 年初我们又证明了初等微分几何中主要的一类定理证明也可以机械化．而且这种机械化方法也是切实可行的，并据此用手算证明了不算简单的一些定理．

从我们的工作中可以看出，定理的机械化证明，往往极度繁复，与通常既简且妙的证明形成对照，这种以量的复杂来换取质的困难，正是利用计算机所需要的．

在电子计算机如此发展的今天，把我们的机械化方法在计算机上实现不仅不难，而且有一台微型的台式机也就够了．就像我们曾经使用过的长城 203，它的存数最多只能到 234 个 10 进位的 12 位数，就已能用以证明西摩松线那样的定理．随着超大规模集成电路与其它技术的出现与改进，微型机将愈来愈小型化而内存却愈来愈大，功能愈来愈多，自动化的程度也愈来愈高．进入 21 世纪以后，这一类方便的小型机器将为广大群众普遍使用．它们不仅将成为证明一些不很简单的定理的武器，而且还可用以发现并证明一些艰深的定理，而这种定理的发现与证明，在数学研究手工业式的过去，将是不可想象的．这里我们应该着重指出，我们并不鼓励以后人们将使用计算机来证明甚至发现一些有趣的几何定理．恰恰相反，我们希望人们不再从事这种虽然有趣却即是对数学甚至几何学本身也已意义不大的工作，而把自己从这种工作中解放出来，把自己的聪明才智与创造能力贯注到更有意义的脑力劳动上去．

还应该指出，目前我们所能证明的定理，局限于已经发现的机械化方法的范围，例如初等几何与初等微分几何之内．而如何超出与扩大这些机械化的范围，则是今后需要探索的长期的理论性工作．

4．历史的启示与中国古代数学

我们发现几何定理证明的机械化方法是在 1976 至 1977 年之间．约在两年之后，我们发现早在 1899 年出版的希尔伯特的经典名著《几何基础》中，就有着一条真正的正面的机械化定理：初等几何中只涉及从属与平行关系的定理证明可以机械化．当然，原来的叙述并不是以机械化的语言来表达的，也许就连希尔伯特本人也并没有对这一定理的机械化意义有明确的认识，自然更不见得有其他人提到过这一定理的机械化内容．希尔伯特是以公理化的典范而著称于世的，但我认为，该书更重要处，是在于提供了一条从公理化出发，通过代数化以到达机械化的道路．自然，处于希尔伯特以及其后数学的一张纸一支笔的手工作业时代里，公理化的思想与方法得到足够的重视与充分的发展，而机械化的方向与意义受到数学家的忽视是完全可以理解的．但在电子计

算机已日益普及，因而繁琐而重复的计算已成为不足道的现代，机械化的思想应比公理化思想受到更大重视，似乎是合乎实际的.

其次应该着重指出，我们在从事机械化定理证明工作获得成果之前，对塔斯基的已有工作并无接触，更没有想到希尔伯特的《几何基础》会与机械化有任何关系. 我们是在中国古代数学的启发之下提出问题并想出解决办法来的.

说起来道理也很简单：中国的古代数学基本上是一种机械化的数学. 四则运算与开方的机械化算法由来已久. 汉初完成的《九章算术》中，对开平、立方与解线性联立方程组的机械化过程，都有详细说明. 宋代更发展到高次代数方程求数值解的机械化算法.

总之各个数学领域都有定理证明的问题，并不限于初等几何或微分几何. 这种定理证明肇始于古希腊的欧几里得传统，现已成为近代纯粹数学或核心数学的主流. 与之相异，中国的古代学者重视的是各种问题特别是来自实际要求的具体问题的解决. 各种问题的已知数据与要求的数据之间，很自然地往往以多项式方程的形式出现. 因之，多项式方程的求解问题，也就自然成为中国古代数学家研究的中心问题. 从秦汉以来，所研究的方程由简到繁，不断有所前进，有所创新. 到宋元时期，更出现了一个思想与方法的飞跃：天元术的创立.

“天元术”到元代朱世杰时又发展成四元术，所引入的天元、地元、人元、物元实际上相当于近代的未知元或未知数. 将这些未知元作为通常的已知数那样加减乘除，就可得到与近代多项式与有理函数相当的概念与相应的表达形式与运算法则. 一些几何性质与关系很容易转化成这种多项式或有理函数的形式及其关系. 这使得过去依题意列方程这种无法可循需要高度技巧的工作从此变成轻而易举. 朱世杰 1303 年的《四元玉鉴》又给出了解任意多至四个未知元的多项式方程组的方法. 这里限于 4 个未知元只是由于所使用的计算工具（算筹和算板）的限制. 实质上他解方程的思想路线与方法完全可以适用于任意多的未知元.

不问可知，在当时的具体条件下，朱世杰的方法有许多缺陷. 首先，当时还没有复数的概念，因之朱世杰往往限于求出（正）实值. 这无可厚非，甚至在 17 世纪笛卡儿的时代也还往往如此. 但此外朱世杰在方法上也未臻完善. 尽管如此，朱世杰的思想路线与方法步骤是完全正确的，我们在上世纪 70 年代之末，遵循朱世杰的思想与方法的基本实质，采用美国数学家里特 (Ritt) 在 1932, 1950 年关于微分方程代数研究书中所提供的某些技术，得出了解任意复多项式方程组的一般算法，并给出了全部复数解的具体表达形式. 此后又得出了实系数时求实解的方法，为重要的优化问题提供了一个具体的方

法.

由于多种问题往往自然导致多项式方程组的求解, 因而我们解方程的一般方法可被应用于形形色色的问题. 这些问题可以来自数学自身, 也可以来自其它自然科学或工程技术. 在本丛书的第一本, 吴文俊 的《数学机械化 —— 方程与几何问题求解》一书中, 可以看到这些应用的实例. 工程技术方面的应用, 在本丛书中有高小山的《几何自动作图与智能 CAD 》与陈发来和冯玉瑜等的《代数曲面造型》两本专著. 上述解多项式方程组的一般方法已推广至代微分方程的情形. 许多应用以及相应论著正在酝酿之中.

5. 未来的技术革命与时代的使命

宋元时代天元术与四元术的创造, 把许多问题特别是几何问题转化成代数方程与方程组的求解问题. 这一方法用于几何可称为几何的代数化. 12 世纪的刘益将新法与“古法”比较, 称“省功数倍”. 这可以说是减轻脑力劳动使数学走上机械化道路的一项伟大的成就.

与天元术的创造相伴, 宋元时代的数学又引进了相当于现代多项式的概念, 建立了多项式的运算法则和消元法的有关代数工具, 使几何代数化的方法得到了有系统的发展, 具见于宋元时代幸以保存至今的杨辉、李冶、朱世杰的许多著作之中. 几何的代数化是解析几何的前身, 这些创造使我国古代数学达到了又一个高峰. 可以说, 当时我国已到达了解析几何与微积分的大门, 具备了创立这些数学关键领域的条件, 但是各种原因使我们数学的雄伟步伐就在这些大门之前停顿下来. 几百年的停顿, 使我们这个古代的数学大国在近代变成了数学上的纯粹入超国家. 然而, 我国古代机械化与代数化的光辉思想和伟大成就是无法磨灭的. 本人关于数学机械化的研究工作, 就是在这些思想与成就启发之下的产物, 它是我国自《九章算术》以迄宋元时期数学的直接继承.

恩格斯曾经指出, 枪炮的出现消除了体力上的差别, 使中世纪的骑士阶级从此消声匿迹, 为欧洲从封建时代进入到资本主义时代准备了条件. 近年有些计算机科学家指出, 个人用计算机的出现, 其冲击作用可与枪炮的出现相比. 枪炮使人们在体力上难分强弱, 而个人用计算机将使人们在智力上难分聪明愚鲁. 又有人对数学的未来提出看法, 认为计算机的出现, 将使数学现在一张纸一支笔的方法, 在历史的长河中, 无异于石器时代的手工方法. 今天的数学家们, 不得不面对计算机的挑战, 但是, 也不必妄自菲薄. 大量繁复的事情交给计算机去做了, 人脑将仍然从事富有创造性的劳动.

我国在体力劳动的机械化革命中曾经掉队, 以致造成现在的落后状态. 在当前新的一场脑力劳动的机械化革命中, 我们不能重蹈覆辙. 数学是一种典型的脑力劳动, 它的机械化有着许多其它类型脑力劳动所不及的有利条件. 它的

发扬与实现对我国的数学家是一种时代的使命. 我国古代数学的光辉, 都鼓舞着我们为实现数学的机械化, 在某种意义上也可以说是真正的现代化而勇往直前.

吴文俊

2002 年 6 月于北京

前　　言

多项式消元技术从经典理论到现代算法经历了颇为崎岖曲折的发展过程. 这一点从范德瓦尔登 消去 其经典著作《近世代数学》早期版本中的“消去理论”一章，威尔希望从代数几何学中消去消去理论的最后痕迹，以及阿比杨卡建议消去消去理论的消去者这些文字游戏里可见一斑. 多项式消元的复兴与广泛认同极大地归功于现代先进计算技术的出现和不断更新. 基于这些技术，有效的算法得以实施，并被用于形形色色的科学与工程问题. 在过去的 20 年里，理论和实际工作者都越来越意识到消去法及其奠基理论的意义和效用. 大量研究活动使这一学科中的算法设计与软件开发突飞猛进，这一点已广为人知. 它们的应用遍及纯数学、应用数学、几何造型、机器人以及人工神经网络.

本书系统地介绍计算多元多项式系统零点分解的消去算法. 其中心概念是各种三角列与三角系统，用以表示这些零点分解. 理解这些概念和算法的预备知识乃是一些基本代数结果和算法数学的常识. 部分贯穿全书有关多元多项式运算的结果罗列于第一章. 第二至第五章致力于描述零点分解算法. 我们首先介绍分解任意多项式系统为三角系统的算法；此时并不保证三角系统总有零点. 这些算法在第三章中通过计算条件最大公因子得以修改扩充，使所求的三角系统为正则或简单的，因而总有零点. 然后，我们阐述如何并入投影过程，以及如何使用多项式因子分解以计算不可约三角系统. 这些算法及其奠基理论的提出与发展则依据里特、吴文俊、赛登贝格和托马斯的工作. 在第五章中，我们对基于结式和格罗布讷基的算法作简单介绍. 消去法在构造性代数几何与多项式理想论中扮演特殊角色. 第六章着重探讨该领域中的几个问题. 本书的最后三章论述符号消去法的若干应用，包括代数方程求解、几何定理求证、以及多项式因子分解与微分系统的定性分析.

本书中的大部分算法都已由笔者在 Maple 系统中实施，它们应在迄今为止最有效的消去算法之列. 这些算法的描述都很形式化，其目的是让读者能据此直接编制自己的软件. 然而，实施细节和理论计算复杂性都未能在书中具体论及.

本书中的材料大部分取自施普林格出版的《消去法》一书[91]和笔者指导研究资格的学位论文[89]，而中文版的结构与表述则有所改进. 书中的部分内容曾由笔者在奥地利开普勒大学符号计算研究所的研究生课程中讲授过多次.

致　谢

笔者衷心感谢恩师吴文俊教授: 他将我引入多项式消元这一迷人的学科, 教会我他的特征列方法, 并予我以数年的指导. 吴先生的工作和思想对我影响如此深远, 以至于我在大部分研究论文中都对此多次提及.

笔者非常感激布鲁诺·布赫贝格尔教授 —— 我从他那里所学到的远远超出了格罗布讷基. 他的慷慨扶持与各种方式的帮助使我多年来工作和生活都轻松自在.

我的许多同事、学生和朋友都给我提供了不同形式的帮助, 比如邀请我去访问、演讲或者简单地共进晚餐, 在我的语言不够用时予以协助, 在我的计算机出故障时伸出援手. 在这里, 我无法列出所有姓名 —— 我谨向他们致以诚挚的谢意.

对里卡尔多·卡费拉教授领导的自动推理小组和达尼埃尔·拉扎尔教授领导的计算机代数专题组的成员, 我应该特别致谢. 他们建立了非常理想的工作环境, 使我能乐在其中, 尽享思考、写作、编程之雅趣.

王东明

2001 年 8 月于巴黎

符 号 表

$\triangleq$	“定义为”
$\prec$, $\succ$	变元序，项序，多项式和三角列的秩序
$\precsim$, $\succsim$, $\sim$	多项式和三角列的秩序
$\backsim$	多项式的相似
$\sqrt{\ }$	(理想的) 根
$\Longleftrightarrow$	“当且仅当”
$\rightsquigarrow$	“简化为”
$\Rightarrow$, $\vee$, $\wedge$	逻辑“蕴涵”，“或”，“和”
$\mathbf{A}^n_{\tilde{\mathcal{K}}}$	$\tilde{\mathcal{K}}$ 上的 n 维仿射空间
$\mathbf{C}$	复数域
cls	多项式的类
coef	多项式关于某项的系数
cont	多项式关于某一变元的容度
deg	多项式关于某一变元的次数
det	方阵的行列式
Dim	代数簇、多项式组或多项式系统的维数
dim	完美三角列或三角系统的维数
GB	多项式组的约化格罗布讷基
gcd	一组多项式，或者两个多项式关于某一变元的最大公因子
Ideal	一组多项式生成的理想
ini	多项式的初式；或者一组多项式的初式的集合
ITS	多项式组或多项式系统的不可约三角序列
$\mathcal{K}$	特征为 0 的数域
$\tilde{\mathcal{K}}$	$\mathcal{K}$ 的扩域
$\tilde{\mathcal{K}}$-Zero	多项式组或多项式系统在 $\tilde{\mathcal{K}}$ 中所有零点的集合
$\bar{\mathcal{K}}$	$\mathcal{K}$ 的代数闭包
$\mathcal{K}(\theta)$	从 $\mathcal{K}$ 通过添加 θ 所得的扩域
lc	多项式 (关于某一变元) 的导系数
ldeg	多项式的导次数
level	多项式组或多项式系统的级
lm	多项式的导项式

lt	多项式的导项
lv	多项式的导元
op	多元组或 (有序) 集合中的第 i 个元素
$\mathbb{P}$	多项式组 (即有限多个非零多项式构成的集合)
$\mathbb{P}^{(i)}$	$\mathbb{P}\cap\mathcal{K}[x_1,\cdots,x_i]$
$\mathbb{P}^{[i]}$	$\mathbb{P}\setminus\mathbb{P}^{(i)}$
$\mathbb{P}^{\langle i\rangle}$	$\mathbb{P}^{(i)}\setminus\mathbb{P}^{(i-1)}$
$\mathbb{P}^{\langle\bar{x},i\rangle}$	$\mathbb{P}\|_{x_1=\bar{x}_1,\cdots,x_i=\bar{x}_i}$
$[\mathbb{P},\mathbb{Q}]$, $\mathfrak{P}$	多项式系统 (即一对多项式组)
$\mathfrak{P}^{(i)}$	$[\mathbb{P}^{(i)},\mathbb{Q}^{(i)}]$, 若 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$
$\mathfrak{P}^{\langle i\rangle}$	$[\mathbb{P}^{\langle i\rangle},\mathbb{Q}^{\langle i\rangle}]$, 若 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$
$\mathfrak{P}^{\langle\bar{x},i\rangle}$	$[\mathbb{P}^{\langle\bar{x},i\rangle},\mathbb{Q}^{\langle\bar{x},i\rangle}]$, 若 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$
$\breve{\mathfrak{P}}$	$\mathbb{P}\cup\mathbb{Q}$, 若 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$
PB	不可约三角列的素基
pp	多项式关于某一变元的本原部分
pquo	多项式对某个非零多项式关于某一变元的伪商
prem	多项式对某个非零多项式 (关于某一变元), 或对某个三角列的伪余式; 或者一组多项式对某个非零多项式, 或对某个三角列的伪余式构成的集合
Q	有理数域
R	实数域
$\mathcal{R}$	环
$\mathcal{R}[\boldsymbol{x}]$	系数在 $\mathcal{R}$ 中、变元为 $\boldsymbol{x}$ 的多项式环
Rad	理想的根
red	多项式 (关于某一变元) 的尾式
RegZero	正则列、三角系统或多项式系统的正则零点集
rem	多项式对某组多项式的余式; 或者一组多项式对某组多项式的余式构成的集合
res	两个多项式关于某一变元, 或者一个多项式对某个三角列的结式
RS	多项式组或多项式系统的正则序列
sat	三角列的浸润
sqfr	多项式的最大无平方因子
SS	多项式组或多项式系统的简单序列
$\mathbb{T}$	三角列
$\mathbb{T}^{\{i\}}$	$[T_1,\cdots,T_i]$, 若 $\mathbb{T}=[T_1,\cdots,T_r]$
$[\mathbb{T},\tilde{\mathbb{T}}]$, $\mathfrak{S}$	简单系统
$[\mathbb{T},\mathbb{U}]$, $\mathfrak{T}$	三角系统

tdeg 多项式的全次数

$\boldsymbol{u}$ $(u_1, \cdots, u_d)$, 或 $u_1, \cdots, u_d$

$\mathcal{V}$ 代数簇

$\boldsymbol{x}$ $(x_1, \cdots, x_n)$, 或 $x_1, \cdots, x_n$

$\boldsymbol{x}_i$ $(x_1, \cdots, x_i)$, 或 $x_1, \cdots, x_i$

$\boldsymbol{\xi}$ $(\xi_1, \cdots, \xi_n)$, 或 $\xi_1, \cdots, \xi_n$, 或 $(\boldsymbol{u}, \eta_1, \cdots, \eta_r)$, 或 $\boldsymbol{u}, \eta_1, \cdots, \eta_r$

$\boldsymbol{\xi}_i$ $(\xi_1, \cdots, \xi_i)$, 或 $\xi_1, \cdots, \xi_i$, 或 $(\boldsymbol{u}, \eta_1, \cdots, \eta_i)$, 或 $\boldsymbol{u}, \eta_1, \cdots, \eta_i$

Z 整数环

$\boldsymbol{z}$ $(\boldsymbol{u}, y_1, \cdots, y_r)$, 或 $\boldsymbol{u}, y_1, \cdots, y_r$

$\boldsymbol{z}_i$ $(\boldsymbol{u}, y_1, \cdots, y_i)$, 或 $\boldsymbol{u}, y_1, \cdots, y_i$

Zero 多项式组或多项式系统所有零点的集合

目　　录

第一章 多项式运算与零点

我们首先介绍一些有关多元多项式的基本概念、运算和性质，它们在以后各章中将会用到. 大部分结果的证明见诸于标准代数教科书，因而被略去. 如果参考文献没有给出，建议读者查阅 [71, 72] 和 [41].

1.1 多 项 式

设 $\mathcal{R}$ 为一环， $x_1, x_2, \cdots, x_n$ 为 n 个不属于 $\mathcal{R}$ 的不同符号，称之为 *未定元*, *未知数* 或 *变元*. 我们常将 $x_1, x_2, \cdots, x_i$ 或 $(x_1, x_2, \cdots, x_i)$ 写成 $\boldsymbol{x}_i$, 且命 $\boldsymbol{x} = \boldsymbol{x}_n$. 对于 n 个非负整数 $i_1, i_2, \cdots, i_n$, 我们可作形式幂积

$$\mu = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

并称其为 *项*.

又设 a 为 $\mathcal{R}$ 中的元素，即 $a \in \mathcal{R}$. 称形如

$$\alpha = a\mu = a x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

的表达式为 *单项式*. 我们有时将它写成 $\alpha = a\boldsymbol{x}^{\boldsymbol{i}}$, 其中

$$\boldsymbol{x} = (x_1, \cdots, x_n), \quad \boldsymbol{i} = (i_1, \cdots, i_n).$$

上面的 a 称为 α 的 *系数*. 若 $a \neq 0$, 则说单项式 α 是 *非零的*.

对于 n 元组 $\boldsymbol{i} = (i_1, \cdots, i_n)$, 它的第 l 个分量 i_l 用 $\mathrm{op}(l, \boldsymbol{i})$ 来记. 任意两个由非负整数构成的 n 元组 $\boldsymbol{i}$ 与 $\boldsymbol{j}$ 称为 *不同的*, 如果存在 l $(1 \leq l \leq n)$ 使 $\mathrm{op}(l, \boldsymbol{i}) \neq \mathrm{op}(l, \boldsymbol{j})$. 两个项 $\boldsymbol{x}^{\boldsymbol{i}}$ 与 $\boldsymbol{x}^{\boldsymbol{j}}$ 称为 *不同的*, 如果 $\boldsymbol{i}$ 和 $\boldsymbol{j}$ 不同. 设 $a_1, \cdots, a_t \in \mathcal{R}$, 且 $\boldsymbol{i}_1, \cdots, \boldsymbol{i}_t$ 为 t 个互不相同、由非负整数构成的 n 元组. 我们称有限和

$$P = \sum_{l=1}^{t} a_l \boldsymbol{x}^{\boldsymbol{i}_l} \tag{1.1.1}$$

是系数 $a_1, \cdots, a_t$ 在 $\mathcal{R}$ 中未定元为 $\boldsymbol{x}$ 的 *多项式*. 如果 P 中的所有单项式都为 0, 即 $a_1 = \cdots = a_t = 0$, 那么多项式 P 为 0. 由于单项式 0 可以任意加到一个多项式上或从中抹去，我们假定任意非零多项式 P 中的所有单项式都不

为零，即 $a_1 \neq 0, \cdots, a_t \neq 0$，并称 t 为 P 的 *项数*. 若 $P \in \mathcal{R}$，则称 P 为 *常数*. 今设 $\boldsymbol{x}^{\boldsymbol{i}}$ 为项. 如果存在 $a \in \mathcal{R}$ 且 $a \neq 0$ 使得单项式 $a\boldsymbol{x}^{\boldsymbol{i}}$ 在 P 中出现，则称 a 为 P 关于 $\boldsymbol{x}^{\boldsymbol{i}}$ 的 *系数*，并用 $\mathrm{coef}(P, \boldsymbol{x}^{\boldsymbol{i}})$ 来表示. 否则，$\mathrm{coef}(P, \boldsymbol{x}^{\boldsymbol{i}})$ 定义为 0.

设 P 为一非零多项式，如 (1.1.1) 所示，而 x_k 为任一变元. 我们将 P 关于 x_k 的 *次数* 记为

$$\deg(P, x_k) \triangleq \max_{1 \leq l \leq t} \mathrm{op}(k, \boldsymbol{i}_l).$$

上式中 $\triangleq$ 读作“定义为”. 为方便起见，我们又定义 $\deg(0, x_k) = -1$. P 的 *全次数* 由下式来定义：

$$\mathrm{tdeg}(P) \triangleq \max_{1 \leq l \leq t} \sum_{k=1}^{n} \mathrm{op}(k, \boldsymbol{i}_l).$$

所有项都具有相同全次数的多项式称为是 *齐次的*.

例 1.1.1 下面是一个 $x_1, \cdots, x_4$ 的整系数多项式：

$$F_1 = x_4^2 + x_1 x_4^2 - x_2 x_4 - x_1 x_2 x_4 + x_1 x_2 + 3\, x_2.$$

不难看出

$$\begin{aligned}
&\mathrm{coef}(F_1, x_1 x_2 x_4) = -1, \quad \mathrm{coef}(F_1, x_2 x_4^3) = 0, \\
&\deg(F_1, x_2) = 1, \quad \deg(F_1, x_4) = 2, \\
&\mathrm{tdeg}(F_1) = 3,
\end{aligned}$$

且 F_1 不是齐次的.

设

$$Q = \sum_{l=1}^{s} b_l \boldsymbol{x}^{\boldsymbol{j}_l}$$

为任一其他多项式. 定义 P 与 Q 的 *和* 为

$$P + Q \triangleq \sum_{l=1}^{r} c_l \boldsymbol{x}^{\boldsymbol{k}_l},$$

其中 $\boldsymbol{k}_1, \cdots, \boldsymbol{k}_r$ 是 $\boldsymbol{i}_1, \cdots, \boldsymbol{i}_t, \boldsymbol{j}_1, \cdots, \boldsymbol{j}_s$ 中所有互不相同的 n 元组，

$$c_l = \mathrm{coef}(P, \boldsymbol{x}^{\boldsymbol{k}_l}) + \mathrm{coef}(Q, \boldsymbol{x}^{\boldsymbol{k}_l}), \quad l = 1, \cdots, r.$$

构造 n 元组

$$\boldsymbol{k}_{\boldsymbol{i}_u\boldsymbol{j}_v} = (\mathrm{op}(1,\boldsymbol{i}_u)+\mathrm{op}(1,\boldsymbol{j}_v),\cdots,\mathrm{op}(n,\boldsymbol{i}_u)+\mathrm{op}(n,\boldsymbol{j}_v)),$$
$$u=1,\cdots,t;\ v=1,\cdots,s,$$

并令 $\boldsymbol{k}_1,\cdots,\boldsymbol{k}_r$ 为它们中所有互不相同者. 定义 P 与 Q 的 *积* 为

$$PQ \triangleq \sum_{l=1}^{r} c_l \boldsymbol{x}^{\boldsymbol{k}_l},$$

其中

$$c_l = \sum_{\boldsymbol{k}_{\boldsymbol{i}_u\boldsymbol{j}_v}=\boldsymbol{k}_l} a_u b_v,\quad l=1,\cdots,r.$$

定理 1.1.1 在上面所定义的加法与乘法之下, 所有系数在 $\mathcal{R}$ 中变元为 $\boldsymbol{x}$ 的多项式构成一环.

将系数在 $\mathcal{R}$ 中 n 个变元 $x_1,\cdots,x_n$ 的多项式构成的环记为 $\mathcal{R}[x_1,\cdots,x_n]$, 或简记为 $\mathcal{R}[\boldsymbol{x}]$. 它也称为由 $\mathcal{R}$ 通过添加 $\boldsymbol{x}$ 导出的 *多项式环*. 如果 $\mathcal{R}$ 是交换环, 那么 $\mathcal{R}[\boldsymbol{x}]$ 也是. 特别在 $\mathcal{R}$ 为整数环 $\mathbb{Z}$ 时, $\mathcal{R}[\boldsymbol{x}]$ 成为整系数多项式环.

定理 1.1.2 如果 $\mathcal{R}$ 是一整环, 那么 $\mathcal{R}[\boldsymbol{x}]$ 也是.

记住 n 总表示变元 $\boldsymbol{x}$ 的个数. 我们说多项式是 *一元的*, *二元的* 或 *多元的* 依据 $n=1, n=2$ 或 $n\geq 2$. 相应地, 多项式环 $\mathcal{R}[\boldsymbol{x}]$ 亦被称为 *一元的*, *二元的* 或 *多元的*, 视 n 为 1, 2 或 ≥ 2 而定. 由 $\mathcal{R}$ 通过添加未定元 $\boldsymbol{x}$ 而导出的多元多项式环 $\mathcal{R}[\boldsymbol{x}]$ 也可视为由 $\mathcal{R}$ 通过依次添加未定元 $x_1,x_2,\cdots,x_n$ 而导出的环 $\mathcal{R}[x_1][x_2]\cdots[x_n]$.

定理 1.1.3 多项式环 $\mathcal{R}[x_1]\cdots[x_n]$, $\mathcal{R}[x_{q_1}]\cdots[x_{q_n}]$ 与 $\mathcal{R}[\boldsymbol{x}]$ 是同构的, 这里 $q_1\cdots q_n$ 为 $1\cdots n$ 的任一置换.

因此, 一个多元多项式 $P\in\mathcal{R}[\boldsymbol{x}]$ 也可理解为关于某一固定变元, 譬如 x_n, 系数在 $\mathcal{R}[x_1,\cdots,x_{n-1}]$ 中的一元多项式. 换句话说, 可视 P 为 $\mathcal{R}[\boldsymbol{x}_{n-1}][x_n]$ 中的元素.

多项式组 是由 $\mathcal{R}[\boldsymbol{x}]$ 中有限多个非零多项式所构成的集合. 说到 *多项式系统*, 我们是指一对多项式组 $[\mathbb{P},\mathbb{Q}]$. 作为一般性的约定, 在本书中我们用大写字母如 P,Q,F 表示多项式, 宽体字母如 $\mathbb{P},\mathbb{Q},\mathbb{T}$ 表示多项式组, 哥特体字

母如 $\mathfrak{P}, \mathfrak{T}, \mathfrak{S}$ 表示多项式系统，希腊字母如 Ψ 表示由多项式系统构成的集合或序列.

以下，我们将未定元排成固定的次序:

$$x_1 \prec \cdots \prec x_n.$$

定义 1.1.1　对于任意两个不同的项 $\boldsymbol{x}^{\boldsymbol{i}}$ 与 $\boldsymbol{x}^{\boldsymbol{j}}$, 其中

$$\boldsymbol{i} = (i_1, \cdots, i_n), \quad \boldsymbol{j} = (j_1, \cdots, j_n),$$

我们说 $\boldsymbol{x}^{\boldsymbol{i}}$ 排在 $\boldsymbol{x}^{\boldsymbol{j}}$ *之前* 或 $\boldsymbol{x}^{\boldsymbol{j}}$ 排在 $\boldsymbol{x}^{\boldsymbol{i}}$ *之后*, 记作

$$\boldsymbol{x}^{\boldsymbol{i}} \prec \boldsymbol{x}^{\boldsymbol{j}} \text{ 或 } \boldsymbol{x}^{\boldsymbol{j}} \succ \boldsymbol{x}^{\boldsymbol{i}},$$

如果存在 k $(1 \le k \le n)$, 使得

$$i_k < j_k, \text{ 且 } i_l = j_l \text{ 对 } k < l \le n \text{ 成立}.$$

在 “$\prec$” 之下，所有关于 $\boldsymbol{x}$ 的项以及 $\mathcal{R}[\boldsymbol{x}]$ 中任一非零多项式的单项式都可排列成序. 我们称 “$\prec$” 为项或单项式的 *纯字典序*.

事实上，$\mathcal{R}[\boldsymbol{x}]$ 中任意非零多项式都可以写成 (1.1.1) 的形式，其中

$$a_1 \ne 0, \cdots, a_t \ne 0, \quad a_i \in \mathcal{R},$$
$$\boldsymbol{x}^{\boldsymbol{i}_1} \succ \cdots \succ \boldsymbol{x}^{\boldsymbol{i}_t}.$$

这时，我们称 $\boldsymbol{x}^{\boldsymbol{i}_1}$ 为 P 的 *导项*, $a_1\boldsymbol{x}^{\boldsymbol{i}_1}$ 为 P 的 *导项式*, a_1 为 P 的 *导系数*, 分别记为 $\mathrm{lt}(P)$, $\mathrm{lm}(P)$ 与 $\mathrm{lc}(P)$. 在 $P \notin \mathcal{K}$ 时，我们称使得

$$\deg(P, x_p) > 0 \text{ 或者等价地 } \deg(\boldsymbol{x}^{\boldsymbol{i}_1}, x_p) > 0$$

成立的最大下标 p 为 P 的 *类*, x_p 为 P 的 *导元*, $\deg(P, x_p)$ 为 P 的 *导次数*, 分别记作 $\mathrm{cls}(P)$, $\mathrm{lv}(P)$ 和 $\mathrm{ldeg}(P)$. 用符号表示，我们有

$$\mathrm{lv}(P) = x_{\mathrm{cls}(P)}, \quad \mathrm{ldeg}(P) = \deg(P, \mathrm{lv}(P)).$$

对任意 $P \in \mathcal{K}$ 但 $P \ne 0$, 我们将 P 的 *类*, *导元* 与 *导次数* 分别定义为 0, x_0 与 0, 这里 x_0 为一新变元，其序排在 x_1 之前 (即 $x_0 \prec x_1$).

设 P 为一多项式，其类 $\mathrm{cls}(P) = p > 0$. 那么可视 P 为 x_p 的一元多项式. 对任一其他多项式 $Q \in \mathcal{R}[\boldsymbol{x}]$, 如果 $\deg(Q, x_p) < \mathrm{ldeg}(P)$, 则称 Q 对 P 是 *约化的*. P 关于 x_p 的导系数 $\mathrm{lc}(P, x_p)$ 称为 P 的 *初式*, 记作 $\mathrm{ini}(P)$, 它是 $x_1, \cdots, x_{p-1}$ 的多项式. 定义任意 $P \in \mathcal{K}$ 的 *初式* 为其本身. 对任意多项式组 $\mathbb{P}$, 我们定义

$$\mathrm{ini}(\mathbb{P}) \triangleq \{\mathrm{ini}(P) \colon P \in \mathbb{P}\}.$$

例 1.1.2 按照变元序 $x_1 \prec \cdots \prec x_4$, 例 1.1.1 中的多项式 F_1 可重写为

$$\begin{aligned}F_1 &= x_1x_4^2 + x_4^2 - x_1x_2x_4 - x_2x_4 + x_1x_2 + 3\,x_2\\ &= (x_1+1)\,x_4^2 + (-x_1x_2 - x_2)\,x_4 + x_1x_2 + 3\,x_2.\end{aligned}$$

由此可见

$$\begin{aligned}&\mathrm{lc}(F_1) = 1,\\ &\mathrm{lt}(F_1) = \mathrm{lt}(F_1) = x_1x_4^2,\\ &\mathrm{cls}(F_1) = 4,\ \ \mathrm{lv}(F_1) = x_4,\\ &\mathrm{ldeg}(F_1) = 2,\ \ \mathrm{ini}(F_1) = x_1 + 1.\end{aligned}$$

多项式

$$F_2 = x_1x_4 + x_3 - x_1x_2$$

对 F_1 是约化的, 但 F_1 对 F_2 不是约化的.

1.2 最大公因子、伪除与多项式余式序列

以下将 $\mathcal{R}$ 限定为唯一析因整环, 即带有单位元的交换环. 这时, 对 $\mathcal{R}$ 中的任意非零元素 a 和 b 都有 $ab \neq 0$, 并且每个 $a \in \mathcal{R}$ 或为"可逆元"或有如下形式的"唯一"表示:

$$a = up_1\cdots p_t,\quad t \geq 1,$$

式中 $p_1, \cdots, p_t$ 为"素数", u 为一可逆元. 每个域都是唯一析因整环, 其中每个非零元素都是可逆元, 但无素数. 若 $\mathcal{R}$ 被假定为唯一析因整环, 那么根据定理 1.1.2 $\mathcal{R}[\boldsymbol{x}]$ 也是唯一析因整环.

设 F 与 G 为 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式, 且 $G \neq 0$. 我们说 G 整除 F 或 F 能被 G 除尽, 记作 $G \mid F$, 如果存在商多项式 $Q \in \mathcal{R}[\boldsymbol{x}]$ 使 $F = QG$. 这时, 称 G 为 F 的因子, F 为 G 的倍数.

定义 1.2.1 设 $P_1, \cdots, P_s$ 为 $\mathcal{R}[\boldsymbol{x}]$ 中不全为 0 的多项式. 如果多项式 $G \in \mathcal{R}[\boldsymbol{x}]$ 整除所有 $P_1, \cdots, P_s$ 并且 $P_1, \cdots, P_s$ 的每个公因子都整除 G, 则称 G 为 $P_1, \cdots, P_s$ 的最大公因子.

如果 $P_1, \cdots, P_s$ 都整除某一多项式 $L \in \mathcal{R}[\boldsymbol{x}]$ 且 L 整除 $P_1, \cdots, P_s$ 的每个公倍数, 则称 L 为 $P_1, \cdots, P_s$ 的最小公倍数.

该定义中的多项式 G 是不唯一的：对任意可逆元 a, aG 也是最大公因子. 但根据唯一析因整环的性质，任意两个最大公因子只相差一个可逆元因子. 所以，可将 $P_1,\cdots,P_s$ 的所有最大公因子看作是恒同的. 对最小公倍数也是如此. 令 $\mathbb{P}=\{P_1,\cdots,P_s\}$.

$$\gcd(\mathbb{P})=\gcd(P_1,\cdots,P_s) \text{ 与 } \mathrm{lcm}(\mathbb{P})=\mathrm{lcm}(P_1,\cdots,P_s)$$

分别表示 $P_1,\cdots,P_s$ 的 *最大公因子* 与 *最小公倍数*.

例 1.2.1 考虑多项式

$$\begin{aligned}G_1&=3\,x_4^2-3\,x_2x_4+6\,x_1x_4-3\,x_3x_4+3\,x_2x_3-6\,x_1x_3,\\ G_2&=6\,x_4^2+15\,x_1x_2x_4-6\,x_3x_4-15\,x_1x_2x_3.\end{aligned}$$

可以验证 $3\,x_3-3\,x_4$ 整除 G_1 与 G_2. 实际上，x_4-x_3 (乘上任一常数) 是 G_1 和 G_2 在 $\mathbb{Q}[x_1,\cdots,x_4]$ 中的最大公因子，这里 $\mathbb{Q}$ 表示有理数域.

设 F 为 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式，而 x_k 为一固定变元. 作为 x_k 的多项式，F 可以写成

$$\begin{aligned}F&=F_0x_k^m+F_1x_k^{m-1}+\cdots+F_m,\\ &\qquad F_i\in\mathcal{R}[x_1,\cdots,x_{k-1},x_{k+1},\cdots,x_n],\end{aligned}$$

这里 $m=\deg(F,x_k)$. 上式中，F_{m-i} 称为 F 关于 x_k^i 的 *系数*, 记作 $\mathrm{coef}(F,x_k^i)$. 特别 F_0 是 F 关于 x_k 的 *导系数*, 记作 $\mathrm{lc}(F,x_k)$. 于是

$$\mathrm{lc}(F,x_k)=\mathrm{coef}(F,x_k^{\deg(F,x_k)}).$$

多项式 $F-F_0x_k^m$ 称为 F 关于 x_k 的 *尾式*, 记作 $\mathrm{red}(F,x_k)$. 在 $x_k=\mathrm{lv}(F)$ 时，x_k 将从 $\mathrm{red}(F,x_k)$ 中略去. 用符号来表示，我们有

$$\begin{aligned}&\mathrm{lc}(F,x_k)\triangleq F_0,\\ &\mathrm{red}(F,x_k)\triangleq F_1x_k^{m-1}+\cdots+F_m,\\ &\mathrm{red}(F)\triangleq\mathrm{red}(F,\mathrm{lv}(F)).\end{aligned}$$

$F_0,\cdots,F_m$ 的最大公因子 —— 视作 $\mathcal{R}[x_1,\cdots,x_{k-1},x_{k+1},\cdots,x_n]$ 中的多项式 —— 称为 F 关于 x_k 的 *容度*, 记为 $\mathrm{cont}(F,x_k)$. 如果 $\mathrm{cont}(F,x_k)$ 是 $\mathcal{R}$ 中的可逆元, 则说 F 关于 x_k 是 *本原的*. 对任意非零多项式 F, 称 $F/\mathrm{cont}(F,x_k)$ 为 F 关于 x_k 的 *本原部分*, 记作 $\mathrm{pp}(F,x_k)$; 于是 F 可以写成

$$F=\mathrm{cont}(F,x_k)\cdot\mathrm{pp}(F,x_k).$$

引理 1.2.1 (高斯引理) **唯一析因整环上本原多项式的积仍是本原的.**

设 $F \neq 0$ 且 $m = \deg(F, x_k)$ 如上, 而 G 为任一其他多项式, 它关于 x_k 的次数为 l. 视为 x_k 的多项式, 用 F 对 G 作伪除, 我们有如下伪除算法. 命 $R = G$; 重复下面的过程直至 $r = \deg(R, x_k) < m$:

$$R \leftarrow F_0 R - R_0 x_k^{r-m} F,$$

其中 $R_0 = \mathrm{lc}(R, x_k)$. 由于 r 在每个循环中都严格下降, 该程序必定终止. 最后得到两个 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式 Q 与 R 满足下列关系:

$$I^q G = QF + R, \tag{1.2.1}$$

这里

$$I = \mathrm{lc}(F, x_k), \quad q = \max(l - m + 1, 0),$$
$$\deg(R, x_k) < m, \quad \deg(Q, x_k) = \max(l - m, -1).$$

在 $m = 0$ 时, $R = 0$, 而 $Q = F^l G$.

我们称表达式 (1.2.1) 为 *伪余公式*; Q 为 G 对 F 关于 x_k 的 *伪商*, R 为 G 对 F 关于 x_k 的 *伪余式*, 分别记为 $\mathrm{pquo}(G, F, x_k)$ 与 $\mathrm{prem}(G, F, x_k)$. 实际上, (1.2.1) 式中的多项式 Q 和 R 由 F 与 G 唯一确定. 现将这一事实叙述如下供以后使用.

命题 1.2.2 设多项式 F, G, I, Q, R 及整数 q 如上. 如果 Q' 与 R' 为 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式, 使得

$$I^q G = Q'F + R',$$

则 $Q' = Q$, 且 $R' = R$.

证 见 [41] 中 402 和 407 页. □

通过用 F 对 G (关于 x_k) 作伪除获得 Q 与 R 的过程称为 *伪约化*. 它是本书中许多算法的基础, 因而将在以后各章中担任关键角色. 由于这一原因, 我们将计算伪余式的过程表述成如下形式的算法.

算法 prem: $R \leftarrow \mathrm{prem}(G, F, x)$. 任给多项式 $G, F \in \mathcal{R}[\boldsymbol{x}]$ 及变元 $x \in \{\boldsymbol{x}\}$, 本算法计算 G 对 F 关于 x 的伪余式 R.

P1. 命 $R \leftarrow G$, $r \leftarrow \deg(R, x)$, $H \leftarrow F$, $h \leftarrow \deg(H, x)$, $d \leftarrow r - h + 1$.

P2. 若 $h \le r$, 则命 $L \leftarrow \mathrm{lc}(H, x)$, $H \leftarrow \mathrm{red}(H, x)$; 否则命 $L \leftarrow 1$.

P3. 重复下列步骤直至[①] $r < h$ 或 $R = 0$:

P3.1. 计算 $T \leftarrow x^{r-h}\mathrm{lc}(R, x)H$.

P3.2. 命 $R \leftarrow \mathrm{red}(R, x)$.

P3.3. 计算 $R \leftarrow LR - T$, 且命 $r \leftarrow \deg(R, x)$, $d \leftarrow d - 1$.

P4. 输出 $R \leftarrow L^d R$.

在 $x_k = \mathrm{lv}(F)$ 时, 变元 x_k 将从 $\mathrm{prem}(G, F, x_k)$ 中略去. 对任一多项式组 $\mathbb{Q}$, $\mathrm{prem}(\mathbb{Q}, F)$ 表示 $\{\mathrm{prem}(Q, F)\colon\ Q \in \mathbb{Q}\}$. 下面给出用作演示伪除过程的简单例子和较复杂的计算例子.

例 1.2.2　考虑多项式

$$F = xy^2 + 1,\quad G = 2\,y^3 - y^2 + x^2 y.$$

关于 y, 相应的 R 和 Q 可如下计算:

$$\begin{array}{lrr}
 & 2\,xy - x & = Q \\
xy^2 + 1 & \overline{)\ 2\,y^3 - y^2 + x^2 y} & G \\
 & 2\,xy^3 - xy^2 + x^3 y & xG \\
 & \underline{-(2\,xy^3 + 2\,y)} & -2\,yF \\
 & -\,xy^2 + x^3 y - 2\,y & \bar{R} \\
 & -\,x^2y^2 + x^4 y - 2\,xy & x\bar{R} \\
 & \underline{-(-x^2y^2 - x)} & xF \\
 & x^4 y - 2\,xy + x & = R.
\end{array}$$

由此即得

$$x^2 G = (2\,xy - x)\,F + x^4 y - 2\,xy + x. \tag{1.2.2}$$

可将公式 (1.2.1) 中的整数 q 定得尽可能小, 只要伪除过程不给 Q 和 R 引进分式即可. 对 prem 的某些应用, 步骤 P4 中的乘式 L^d 可被略去. 在 (1.2.2) 中, 也可取 $q = 1$ 代替 2 使其简化为

$$xG = (2\,y - 1)\,F + x^3 y - 2y + 1.$$

---

① 一旦条件 “$r < h$ 或 $R = 0$” 满足便停止执行.

在实际计算时，选取最小的 q 对控制伪余式的扩大乃至关重要. 而且，可以通过用 $I_1^{q_1}\cdots I_e^{q_e}$ 替代 I^q 对公式 (1.2.1) 加以修正，这里 $I_1,\cdots,I_e$ 是 I 的所有互异不可约因子 (关于不可约的定义，参见 1.4 节)，并取最小的 $q_1,\cdots,q_e$ 使相应的伪余公式仍然成立. 对于这一修正，R 的确定需要附加计算，因而在每步中占用更多的时间. 然而，修正后的伪除法可以避免一些多余的因子而使后面的计算受益.

例 1.2.3 考虑例 1.1.1, 1.1.2 与 1.2.1 中给出的多项式 F_1,F_2, G_1,G_2. 用 F_2 对 F_1 关于 x_4 作伪除可得下面的伪余公式:

$$x_1^2F_1 = QF_2 + R,$$

其中

$$\begin{aligned}
Q &= x_1^2x_4 + x_1x_4 - x_1x_3 - x_3,\\
R &= \mathrm{prem}(F_1,F_2) = x_1x_3^2 + x_3^2 - x_1^2x_2x_3 - x_1x_2x_3 + x_1^3x_2 + 3\,x_1^2x_2.
\end{aligned}$$

也可以验证

$$\begin{aligned}
G_3 &= \mathrm{prem}(G_1,G_2,x_4)\\
&= -45\,x_1x_2x_4 - 18\,x_2x_4 + 36\,x_1x_4 + 45\,x_1x_2x_3 + 18\,x_2x_3 - 36\,x_1x_3,\\
G_3' &= \mathrm{prem}(F_1,G_2,x_4)\\
&= 6\,x_1x_3x_4 + 6\,x_3x_4 - 15\,x_1^2x_2x_4 - 21\,x_1x_2x_4 - 6\,x_2x_4 + 15\,x_1^2x_2x_3\\
&\quad + 15\,x_1x_2x_3 + 6\,x_1x_2 + 18\,x_2,
\end{aligned}$$

以及

$$\begin{aligned}
&\mathrm{cont}(F_1,x_4) = 1,\\
&\mathrm{cont}(G_1,x_4) = \mathrm{cont}(G_2,x_4) = \mathrm{cont}(G_3',x_4) = 3,\\
&\mathrm{cont}(G_3,x_4) = 45\,x_1x_2 + 18\,x_2 - 36\,x_1,\\
&\mathrm{pp}(G_3,x_4) = x_3 - x_4.
\end{aligned}$$

两个多项式 $F,G\in\mathcal{R}[x]$ 称为 *相似的*，记作 $F\backsim G$，如果存在 $a,b\in\mathcal{R}$, $ab\neq 0$，使得 $aF=bG$.

将多项式 G 和 F 更名为 P_1 和 P_2，并假定 $\deg(P_1,x_k)\geq\deg(P_2,x_k)$. 作多项式序列

$$P_1,P_2,P_3,\cdots,P_r$$

使得

$$P_i \backsim \mathrm{prem}(P_{i-2},P_{i-1},x_k),\quad i=3,\cdots,r$$

且

$$\mathrm{prem}(P_{r-1}, P_r, x_k) = 0.$$

这样的序列称为 G 和 F 关于 x_k 的 *多项式余式序列*.

从伪余公式及多项式余式序列的构造可以看出

$$\gcd(P_1, P_2), \gcd(P_2, P_3), \cdots, \gcd(P_{r-1}, P_r), P_r$$

之间只相差 $\mathcal{R}[x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n]$ 中的多项式因子. 如果 P_1 和 P_2 关于 x_k 都是本原的, 则

$$\gcd(G, F) = \gcd(P_1, P_2) = \mathrm{pp}(P_r, x_k).$$

另一方面, 容易看出

$$\gcd(G, F) = \gcd(\mathrm{cont}(G, x_k), \mathrm{cont}(F, x_k)) \cdot \gcd(\mathrm{pp}(G, x_k), \mathrm{pp}(F, x_k))$$

对任意多项式 G 和 F 成立. 因而, 构造多项式余式序列为求两个多项式的最大公因子提供了一种手段; 而求多个多项式的最大公因子可以很容易地归结到两个多项式的情形.

例 1.2.4 考虑例 1.2.1 中的多项式. 经算法 prem 计算表明

$$\begin{aligned}
&\mathrm{prem}(G_2, G_3, x_4) = 0,\\
G_4' &= \mathrm{prem}(G_2, G_3', x_4)\\
&= 2430\, x_1^2x_2^2x_3^2 + 3240\, x_1^3x_2^2x_3^2 - 2430\, x_1^2x_2^3x_3 + 864\, x_1x_2x_3^2\\
&\quad - 540\, x_1x_2^3x_3 + 216\, x_1^2x_2x_3^2 + 1350\, x_1^4x_2^2x_3^2 - 216\, x_1^2x_2^2x_3\\
&\quad - 3240\, x_1^3x_2^3x_3 - 1350\, x_1^4x_2^3x_3 + 540\, x_1x_2^2x_3^2 - 864\, x_1x_2^2x_3\\
&\quad + 1296\, x_1x_2^2 + 216\, x_1^2x_2^2 + 6210\, x_1^2x_2^3 + 5940\, x_1^3x_2^3 + 1350\, x_1^4x_2^3\\
&\quad + 1620\, x_1x_2^3 - 648\, x_2^2x_3 + 648\, x_2x_3^2 + 1944\, x_2^2,\\
&\mathrm{prem}(G_3', G_4', x_4) = 0.
\end{aligned}$$

因而 G_1, G_2, G_3 和 F_1, G_2, G_3', G_4' 都是多项式余式序列. 由此得出

$$\begin{aligned}
\gcd(G_1, G_2) &= \mathrm{pp}(G_3, x_4) = x_3 - x_4,\\
\gcd(F_1, G_2) &= \mathrm{pp}(G_4', x_4) = 1.
\end{aligned}$$

定义 1.2.2 环 $\mathcal{R}[x]$ 中的非零多项式序列 $P_1, P_2, \cdots, P_r$ 称为 P_1 和 P_2 关于 x 的 *子结式多项式余式序列*, 这里

$$r \geq 2, \quad d_i = \deg(P_i, x), \quad d_1 \geq d_2, \quad I_i = \mathrm{lc}(P_i, x),$$

如果

$$\begin{aligned} P_{i+2} &= \mathrm{prem}(P_i, P_{i+1}, x)/Q_{i+2}, \quad 1 \leq i \leq r-2, \\ &\mathrm{prem}(P_{r-1}, P_r, x) = 0, \end{aligned}$$

这里

$$\begin{aligned} Q_3 &= (-1)^{d_1 - d_2 + 1}, \quad H_3 = -1, \\ Q_i &= -I_{i-2} H_i^{d_{i-2} - d_{i-1}}, \\ H_i &= (-I_{i-2})^{d_{i-3} - d_{i-2}} H_{i-1}^{1 - d_{i-3} + d_{i-2}}, \quad i = 4, \cdots, r. \end{aligned}$$

下一节中，我们将介绍若干有关 *子结式* 的已知结果. 它们确保上面子结式多项式余式序列的定义是合适的，即对所有 $i \geq 3$, 只要 $P_1, P_2 \in \mathcal{R}[x]$ 就有 $P_i \in \mathcal{R}[x]$.

1.3 结式与子结式

两个一元多项式 $F, G \in \mathcal{R}[x]$ 的 *结式* 是关于 F 和 G 的系数的一种形式，该形式为零将为这两个多项式关于 x 有公共零点提供某种条件. 这里 F 和 G 的公共 *零点* $\bar{x}$ 是指 $\mathcal{R}$ 之商域的某一扩域中的数使得 $F(\bar{x}) = G(\bar{x}) = 0$. 它的正式定义将在 1.5 节中给出. 本节的理想参考文献是 [57] 中的第七章.

设 F 和 G 关于 x 的次数分别为 m 和 l, 且 $m \geq l > 0$, 并将 F 与 G 写成

$$\begin{aligned} F &= a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m, \\ G &= b_0 x^l + b_1 x^{l-1} + \cdots + b_{l-1} x + b_l. \end{aligned} \tag{1.3.1}$$

我们构造一个 $m + l$ 阶方阵如下:

$$\mathbf{S} = \left(\begin{array}{cccccccc} a_0 & a_1 & \cdots & a_m & & & & \\ & a_0 & a_1 & \cdots & a_m & & & \\ & & \ddots & \ddots & & \ddots & & \\ & & & a_0 & a_1 & \cdots & a_m & \\ b_0 & b_1 & \cdots & b_l & & & & \\ & b_0 & b_1 & \cdots & b_l & & & \\ & & \ddots & \ddots & & \ddots & & \\ & & & b_0 & b_1 & \cdots & b_l & \end{array} \right) \begin{array}{l} \left.\vphantom{\begin{array}{c} a \\ a \\ a \\ a \end{array}}\right\} l \\ \left.\vphantom{\begin{array}{c} b \\ b \\ b \\ b \end{array}}\right\} m \end{array},$$

其中空白处的元素都为 0. 称该方阵为 F 和 G 关于 x 的 **西尔维斯特矩阵**.

定义 1.3.1 称西尔维斯特矩阵 $\mathbf{S}$ 的行列式为 F 和 G 关于 x 的 **西尔维斯特结式**, 记作 $\mathrm{res}(F,G,x)$.

和往常一样, 我们用 $\det(\square)$ 表示方阵 $\square$ 的 **行列式**. 结式 $\mathrm{res}(F,G,x)=\det(\mathbf{S})$ 是齐次的, 它关于 a_i 的次数为 l, 关于 b_i 的次数为 m.

例 1.3.1 考虑 x 的三次多项式

$$F=ax^3+bx^2+cx+d.$$

F 与其导数

$$\frac{dF}{dx}=3\,ax^2+2\,bx+c$$

的结式 R 也称为 F 的 **判别式**. 若 $a\neq 0$, $F=0$ 有重根的充要条件为 $R=0$.

F 和 dF/dx 关于 x 的 5 阶西尔维斯特矩阵 $\mathbf{S}$ 如下:

$$\mathbf{S}=\begin{pmatrix} a & b & c & d & 0\\ 0 & a & b & c & d\\ 3\,a & 2\,b & c & 0 & 0\\ 0 & 3\,a & 2\,b & c & 0\\ 0 & 0 & 3\,a & 2\,b & c \end{pmatrix}.$$

因而 F 和 dF/dx 关于 x 的西尔维斯特结式为

$$\mathrm{res}(F,dF/dx,x)=\det(\mathbf{S})=a\,(27\,a^2d^2-18\,abcd+4\,b^3d+4\,ac^3-b^2c^2).$$

引理 1.3.1 设 F 和 G 如 (1.3.1) 所示, 则存在多项式 $A,B\in\mathcal{R}[x]$, 使得

$$AF+BG=\mathrm{res}(F,G,x),$$

这里 $\deg(A,x)<\deg(G,x)$, $\deg(B,x)<\deg(F,x)$.

这一引理的证明见于 [72] 中第 85 页和 [57] 中 228 、229 页. 作为以上引理和定义的推论, 我们有下述定理中的充分性.

定理 1.3.2 设 F 和 G 如 (1.3.1) 所示, 则 $\mathrm{res}(F,G,x)=0$ 当且仅当 F 和 G 关于 x 有公共零点, 或者 $a_0=b_0=0$.

该定理中的必要性也不难证明 (见 [72] 第 83 、84 页). 如果 a_0, b_0 之一不为零, 则 $\mathrm{res}(F,G,x)=0$ 是 F 和 G 有公共零点的充要条件.

现设 $\mathbf{S}_{ij}$ 为通过删除矩阵 $\mathbf{S}$ 中 l 行 F 系数中的最后 j 行, m 行 G 系数中的最后 j 行, 和最后 $2j+1$ 列, 但第 $m+l-i-j$ 列除外, 所得的子矩阵, 这里 $0\le i\le j<l$.

定义 1.3.2 对 $0\le j<l$, 多项式

$$S_j(x)=\sum_{i=0}^{j}\det(\mathbf{S}_{ij})x^i$$

称为 F 和 G 关于 x 的第 j 个 *子结式*. 这里 $\deg(S_j,x)\le j$, 并称 $R_j=\det(\mathbf{S}_{jj})$ 为 F 和 G 关于 x 的第 j 个 *主子结式系数*, 或第 j 个 *结式*.

如果 $m>l+1$, 则将 F 和 G 关于 x 的第 j 个 *子结式* $S_j(x)$ 与 *主子结式系数* R_j 的定义拓广如下:

$$S_l(x)=b_0^{m-l-1}G,\quad R_l=b_0^{m-l};\quad S_j(x)=R_j=0,\ l<j<m-1.$$

如果 $\deg(S_j,x)=r<j$, 则称 S_j 为 r 次 *亏损的*; 否则, 称 S_j 为 *正则的*.

容易看出 $S_0=R_0$ 为 F 和 G 关于 x 的 *结式*.

定理 1.3.3 设 F 和 G 为 $\mathcal{R}[x]$ 中的多项式, 且 $m=\deg(F,x)\ge\deg(G,x)=l>0$. 又设 S_j 为 F 和 G 关于 x 的第 j 个子结式, $0\le j<m-1$, 则存在多项式 $A_j,B_j\in\mathcal{R}[x]$, 使得

$$A_jF+B_jG=S_j,$$

这里 $\deg(A_j,x)<l-j$, $\deg(B_j,x)<m-j$.

证 见 [57] 第 255 、256 页. □

定义 1.3.3 设 F 和 G 为 $\mathcal{R}[x]$ 中的多项式, 且 $m=\deg(F,x)\ge\deg(G,x)=l>0$. 令

$$\mu=\begin{cases} m-1 & \text{若 } m>l,\\ l & \text{否则.}\end{cases}$$

又命 $S_{\mu+1}=F$, $S_\mu=G$, 并设 S_j 为 F 和 G 关于 x 的第 j 个子结式, $0\le j<\mu$. 称 $\mathcal{R}[x]$ 中的多项式序列

$$S_{\mu+1}, S_\mu, S_{\mu-1}, \cdots, S_0$$

为 F 和 G 关于 x 的 *子结式链*. 如果所有 S_j 都是正则的, 则称该链为 *正则的*. 否则, 称其为 *亏损的*.

命

$$R_{\mu+1}=1,\quad 而\quad R_j=\begin{cases}\mathrm{lc}(S_j,x) & 若\ S_j\ 是正则的,\\ 0 & 否则,\end{cases}\qquad 0\le j\le\mu.$$

称多项式序列

$$R_{\mu+1}, R_\mu, \cdots, R_0$$

为 F 和 G 关于 x 的 *主子结式系数链*.

这里定义的主子结式系数链与定义 1.3.2 中的主子结式系数是一致的. 事实上, 对 $1\le j<\mu$, 上面的 R_j 即是第 j 个主子结式系数, 它在 S_j 亏损时为零.

定理 1.3.4 (子结式链定理) 设 $S_{\mu+1}$ 和 S_μ 为 $\mathcal{R}[x]$ 中的多项式, 且 $\deg(S_{\mu+1},x)\ge\deg(S_\mu,x)>0$. 又设

$$S_{\mu+1}, S_\mu, \cdots, S_0$$

为 $S_{\mu+1}$ 和 S_μ 关于 x 的子结式链, 其主子结式系数链为

$$R_{\mu+1}, R_\mu, \cdots, R_0.$$

如果 S_{j+1} 和 S_j 都是正则的, 则

$$R_{j+1}^2 S_{j-1}=\mathrm{prem}(S_{j+1},S_j,x),\quad 1\le j\le\mu.$$

如果 S_{j+1} 是正则的, 但 S_j 是 r $(<j)$ 次亏损的, 则

$$\begin{aligned}S_{j-1}=S_{j-2}=\cdots=S_{r+1}=0,&\quad -1\le r<j<\mu,\\ R_{j+1}^{j-r}S_r=\mathrm{lc}(S_j,x)^{j-r}S_j,&\quad 0\le r\le j<\mu,\\ (-1)^{j-r}R_{j+1}^{j-r+2}S_{r-1}=\mathrm{prem}(S_{j+1},S_j,x),&\quad 0<r\le j<\mu.\end{aligned}$$

证 见 [54] 第 122 、123 页，或者 [57] 中 268 及 274—283 页. □

定理 1.3.4 提供了一个用伪除构造子结式链的有效算法. 但在 $\deg(S_{\mu+1}, x) = \deg(S_\mu, x)$ 时，$S_{\mu+1}$ 是亏损的，因而该定理未给出如何求得 $S_{\mu-1}$. 为处理这一特殊情形，我们需要下面的结果. 这一结果在后面也将被用到.

命题 1.3.5 设 ϕ 为 $\mathcal{R}$ 到另一唯一析因整环 $\tilde{\mathcal{R}}$ 上的一个环同态及其诱导的 $\mathcal{R}[x]$ 到 $\tilde{\mathcal{R}}[x]$ 上的环同态，F, G, m, l 如 (1.3.1) 所示，且

$$\tilde{a}_0 = \phi(a_0), \quad \tilde{b}_0 = \phi(b_0), \quad \tilde{m} = \deg(\phi(F), x), \quad \tilde{l} = \deg(\phi(G), x),$$

则关于 x, $\phi(F)$ 和 $\phi(G)$ 的第 j 个子结式 $\tilde{S}_j$ 等同于 F 和 G 的第 j 个子结式 S_j 乘上 δ, 即 $\tilde{S}_j = \delta S_j$, $0 \le j < \max(\tilde{m}, \tilde{l}) - 1$, 这里

$$\delta = \begin{cases} 1 & \text{若 } \tilde{a}_0\tilde{b}_0 \neq 0, \\ \tilde{a}_0^{l-\tilde{l}} & \text{若 } \tilde{a}_0 \neq 0 \text{ 而 } \tilde{b}_0 = 0, \\ \tilde{b}_0^{m-\tilde{m}} & \text{若 } \tilde{a}_0 = 0 \text{ 而 } \tilde{b}_0 \neq 0, \\ 0 & \text{若 } \tilde{a}_0 = \tilde{b}_0 = 0. \end{cases}$$

证 见 [57] 第 264 和 265 页推论 7.8.2. □

现在我们回到子结式链，并将 $S_{\mu+1}$ 视作从一个以未定元为系数，变元为 x, 次数为 $\mu+1$ 的一般多项式 S, 通过将其系数 $\mathrm{lc}(S, x)$ 特定化为 0, $\mathrm{coef}(S, x^i)$ 特定化为 $\mathrm{coef}(S_{\mu+1}, x^i)$, $i = \mu, \cdots, 0$, 所得. 按照命题 1.3.5, $S_{\mu-1}$ 恒同于 S 和 S_μ 关于 x 的第 $\mu - 1$ 个子结式乘上 $\mathrm{lc}(S_\mu, x)$. 由此可知

$$S_{\mu-1} = \mathrm{lc}(S_\mu, x)\,\mathrm{prem}(S_{\mu+1}, S_\mu, x).$$

根据定理 1.3.4 和上面的讨论，我们可以给出如下计算子结式链的算法.

算法 SubresChain: $\mathfrak{S} \leftarrow \mathrm{SubresChain}(F, G)$. 给定多项式 $F, G \in \mathcal{R}[x]$, 这里 $\deg(F, x) \ge \deg(G, x) > 0$, 本算法计算 F 和 G 关于 x 的子结式链 $\mathfrak{S}$.

S1. 命 $m \leftarrow \deg(F, x)$, $l \leftarrow \deg(G, x)$. 如果 $l < m$, 则命 $j \leftarrow m - 1$; 否则命 $j \leftarrow l$. 又命

$$S_{j+1} \leftarrow F, \quad S_j \leftarrow G, \quad R_{j+1} \leftarrow 1, \quad \mu \leftarrow j.$$

S2. 如果 $S_j=0$, 则命 $r\leftarrow -1$; 否则命 $r\leftarrow\deg(S_j,x)$. 对 $k=j-1,j-2,\cdots,r+1$, 命 $S_k\leftarrow 0$.

S3. 如果 $0\le r<j$, 则计算

$$S_r\leftarrow \mathrm{lc}(S_j,x)^{j-r}S_j/R_{j+1}^{j-r}.$$

如果 $r\le 0$, 则输出 $\mathfrak{S}\leftarrow[S_{\mu+1},S_\mu,\cdots,S_0]$, 且算法终止.

S4. 如果 $r=m=l$, 则命 $I\leftarrow\mathrm{lc}(G,x)$; 否则命 $I\leftarrow 1$. 计算

$$S_{r-1}\leftarrow I\,\mathrm{prem}(S_{j+1},S_j,x)/(-R_{j+1})^{j-r+2}.$$

命 $j\leftarrow r-1$, $R_{j+1}\leftarrow\mathrm{lc}(S_{j+1},x)$, 并回到 S2.

例 1.3.2 考虑

$$F=-x^4-z^3x^2+x^2-z^4+2\,z^2-1,$$
$$G=x^4+z^2x^2-r^2x^2+z^4-2\,z^2+1.$$

应用 SubresChain 可得 F 和 G 关于 x 的子结式链如下:

$$F,\ \ G,\ \ -Hx^2,\ \ H^2x^2,\ \ (z^4-2\,z^2+1)\,H^3,\ \ (z^4-2\,z^2+1)^2H^4,$$

其中 $H=z^3-z^2+r^2-1$. 此时 $\mu=4$; S_4,S_2,S_0 是正则的, 而 S_5,S_3,S_1 分别为 4,2,0 次亏损的.

定义 1.3.4 设 $S_{\mu+1}$ 和 S_μ 为 $\mathcal{R}[x]$ 中的多项式, 且 $\deg(S_{\mu+1},x)\ge\deg(S_\mu,x)>0$. 又设

$$\mathfrak{S}:\ S_{\mu+1},S_\mu,\cdots,S_0$$

为 $S_{\mu+1}$ 和 S_μ 关于 x 的子结式链. 严格递减的非负整数序列

$$d_1,d_2,\cdots,d_r$$

称为 $\mathfrak{S}$ 的 *块指标*, 如果 $d_1=\mu+1$, 对任意 $2\le i\le r$, S_{d_i} 都是正则的, 而对 $0\le j\le\mu$, $j\notin\{d_2,\cdots,d_r\}$, S_j 是亏损的.

称正则子结式序列

$$S_{d_2},\cdots,S_{d_r}$$

为 $S_{\mu+1}$ 和 S_μ 关于 x 的 *子结式正则子链*.

子结式链 $\mathfrak{S}$ 具有其块指标 $d_1, \cdots, d_r$ 所刻画的有趣块结构. 它的第一块由单项 $S_{\mu+1}$ 构成. 对任意 $2 \le i \le r$,

$$S_{d_i} \neq 0,\ S_{d_i} \backsim S_{d_{i-1}-1},\ \text{而}\ S_{d_{i-1}-2} = \cdots = S_{d_i+1} = 0.$$

也就是说, $\mathfrak{S}$ 的第 i **非零块** 具有如下形式:

$$S_{d_{i-1}-1}, 0, \cdots, 0, S_{d_i},$$

这里 $S_{d_{i-1}-1} \backsim S_{d_i}$, 且 $d_{i-1} - 1 \ge d_i$. 如果 $d_r > 0$, 则

$$S_{d_r-1} = \cdots = S_0 = 0;$$

这是 $\mathfrak{S}$ 的最后一块, 称之为 **零块**. $\mathfrak{S}$ 的块结构如图 1 所示.

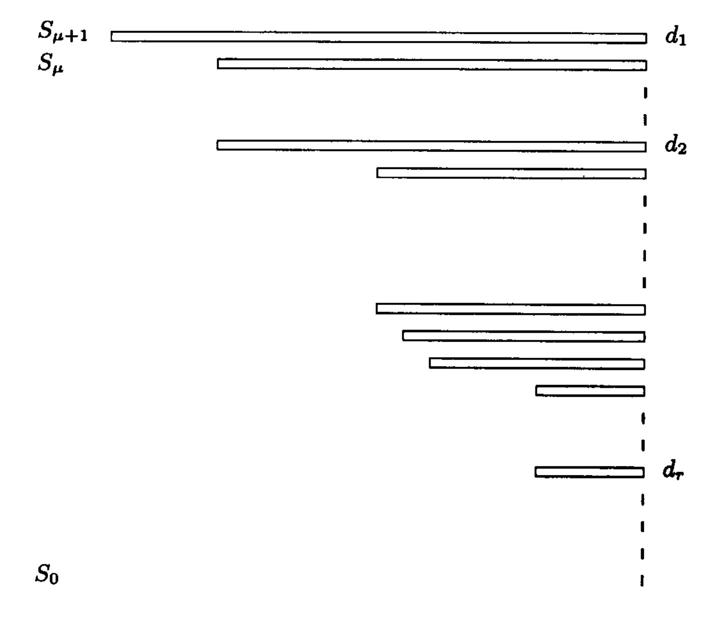


图 1 子结式链的块结构

下面的定理建立了子结式多项式余式序列与子结式链之间的关系, 从而说明子结式多项式余式序列的定义是合适的 (见定义 1.2.2).

定理 1.3.6 设 $S_{\mu+1}, S_\mu, \cdots, S_0$ 和 $d_1, d_2, \cdots, d_r$ 与定义 1.3.4 中相同. 那么多项式序列

$$S_{d_1}, S_{d_1-1}, S_{d_2-1}, \cdots, S_{d_{r-1}-1}$$

为 $S_{\mu+1}$ 和 S_μ 关于 x 的子结式多项式余式序列.

证　见 [19], 或 [57] 第 272 、273 页. □

容易看出,

$$S_{\mu+1}, S_\mu, S_{d_3}, \cdots, S_{d_r}$$

也是 $S_{\mu+1}$ 和 S_μ 关于 x 的多项式余式序列. 因而, 可对算法 SubresChain 加以修改, 用来计算多项式余式序列、子结式多项式余式序列和结式.

例 1.3.3　作为一个较复杂的例子, 考虑

$$\begin{aligned}
P_1 = {} & 729\,y^6 - 1458\,x^3y^4 + 729\,x^2y^4 - 4158\,xy^4 - 1685\,y^4 + 729\,x^6y^2 \\
& - 1458\,x^5y^2 - 2619\,x^4y^2 - 4892\,x^3y^2 - 297\,x^2y^2 + 5814\,xy^2 \\
& + 427\,y^2 + 729\,x^8 + 216\,x^7 - 2900\,x^6 - 2376\,x^5 + 3870\,x^4 \\
& + 4072\,x^3 - 1188\,x^2 - 1656\,x + 529, \\
P_2 = {} & 2187\,y^4 - 4374\,x^3y^2 - 972\,x^2y^2 - 12474\,xy^2 - 2868\,y^2 + 2187\,x^6 \\
& - 1944\,x^5 - 10125\,x^4 - 4800\,x^3 + 2501\,x^2 + 4968\,x - 1587.
\end{aligned}$$

P_1 和 P_2 关于 y 的子结式链 $\mathfrak{S}$ 为

$$\begin{aligned}
S_6 &= P_1, \\
S_5 &= P_2, \\
S_4 &= 2187\,P_2, \\
S_3 &= 1549681956\,x^2(-8748\,x^3y^2 - 8262\,x^2y^2 - 8478\,xy^2 + 498\,y^2 \\
&\quad + 2187\,x^6 - 7776\,x^5 - 18252\,x^4 + 4812\,x^3 + 4787\,x^2 - 540\,x - 2766), \\
S_2 &= -1944\,x^2F_1F_2S_3, \\
S_1 &= 12050326889856\,x^6F_1F_2F_3^2F_4^2, \\
S_0 &= 8033551259904\,x^8F_3^4F_4^4,
\end{aligned}$$

其中

$$\begin{aligned}
F_1 &= 18\,x - 1, \\
F_2 &= 81\,x^2 + 81\,x + 83, \\
F_3 &= 81\,x^2 + 18\,x + 28, \\
F_4 &= 729\,x^4 + 972\,x^3 - 1026\,x^2 + 1684\,x + 765.
\end{aligned}$$

所以, $\mathfrak{S}$ 的块指标为 $6, 4, 2, 0$, 而 S_6, S_5, S_3, S_1 为 P_1 和 P_2 关于 y 的子结式多项式余式序列. 为了简洁与可读性, 我们将上面的某些多项式写成了因子的乘积.

如果 x 被特定化，譬如说，取值 1/18, 那么 F_1 变为 0. 置

$$\bar{S}_j = S_j|_{x=\frac{1}{18}}, \quad j = 6, \cdots, 0,$$

则 $\bar{S}_1 = \bar{S}_2 = 0$, 且 $\bar{S}_0, \bar{S}_3$ 均为常数. 因而，特定化之后子结式链的块指标变成 6,4,0. 应用命题 1.3.5 可知，对任意 j, $\bar{S}_6$ 和 $\bar{S}_5$ 关于 y 的第 j 个子结式恒同于 $\bar{S}_j$. 于是 $\bar{S}_6, \bar{S}_5, \bar{S}_3$ 是 $\bar{S}_6$ 和 $\bar{S}_5$ 关于 y 的子结式多项式余式序列.

基于结式的消去理论是构造性代数中经典消去理论之一，并在现代计算机代数与几何中有广泛应用. 其思想及其发展归功于诸多代数学家，包括欧拉、贝佐、狄克逊、凯莱和西尔维斯特. 较容易的参考文献是 [71, 72] 和 [57] 中的第七章. 在本书的 5.4 节中，我们将说明构造一元结式的另一种方法，并介绍多元结式以及有关的各种消元技术.

经常提到的有关子结式的概念、理论与算法的现代参考文献包括 [19, 20, 6, 41, 54] 以及哈比希特的早期方法. 这里，我们想特别指出托马斯更早的著作 [68, 69], 其中有关概念已被引入.

1.4 域的扩张与因子分解

设 $\mathcal{R}$ 为唯一析因整环. 称多项式 $F \in \mathcal{R}[x]$ 在环 $\tilde{\mathcal{R}}$ ($\supset \mathcal{R}$) 上为 *不可约的*, 如果它不能写成两个 $\tilde{\mathcal{R}}[x]$ 中非常数多项式的乘积. 否则，称 F 在 $\tilde{\mathcal{R}}$ 上是 *可约的*. 在 $\mathcal{R}$ 上，每个多项式都能分解为不可约多项式的乘积；若不计常数因子，其分解是唯一的.

今设 $\mathcal{K}$ 为 $\mathcal{R}$ 的商域. $\mathcal{R}$ 最简单具体的例子是整数环 Z, 此时 $\mathcal{K}$ 成为有理数域 Q. 根据高斯引理 (见 [72] 第 73 页), 如果 $\mathcal{R}[x]$ 中的多项式在 $\mathcal{K}$ 上可分解，那么它在 $\mathcal{R}$ 上也可以分解. 因此，只考虑 $\mathcal{K}$ 上而非 $\mathcal{R}$ 上的因子分解是合适的. 一个非常基本的问题是将 $\mathcal{K}[x]$ 中的任给多项式分解为 $\mathcal{K}[x]$ 中不可约多项式的乘积. 就实际计算而言，这一概念简单的问题并不简单. 然而，各种高效的算法已经存在 (参阅 [41] 中 420–441 页), 并已在流行的计算机代数系统中实现. 所以在需要 $\mathcal{K}$ 上的多项式因子分解时，我们可以自由地使用这些算法和软件系统.

在本书的第四章中，我们将要考虑 $\mathcal{K}[x]$ 中的多项式在 $\mathcal{K}$ 的 *代数扩域* 上的因子分解. 我们现对这一因子分解问题作如下说明.

设 θ 为 $\mathcal{K}$ 的某一扩域 $\tilde{\mathcal{K}}$ 但非 $\mathcal{K}$ 中的元素. $\mathcal{K}(\theta)$ 表示所有有理函数 $F(\theta)/G(\theta)$ 构成的集合，这里 F 和 G 都是系数在 $\mathcal{K}$ 中 θ 的多项式，且 $G(\theta)$ 在 $\tilde{\mathcal{K}}$ 中不为零. 那么在 $\tilde{\mathcal{K}}$ 的运算之下，$\mathcal{K}(\theta)$ 构成一个包含 $\mathcal{K}$ 的数域，称

之为由 $\mathcal{K}$ 通过添加 θ 所得的单扩域. 如果对任意一元多项式 $A \in \mathcal{K}[y]$ 都有 $A(\theta) \neq 0$, 则 θ 是 $\mathcal{K}$ 上的超越数; 这时称 $\mathcal{K}(\theta)$ 为由 $\mathcal{K}$ 通过添加 θ 所得的超越扩域. 在这种情形, 也称 $\mathcal{K}(\theta)$ 为 $\mathcal{K}$ 的有理函数域.

以下我们致力于存在多项式 $A \in \mathcal{K}[y]$ 使 $A(\theta) = 0$ 的情形. 设 A 为这样的多项式, 它关于 y 的次数 m 最小. 这时, θ 是 $\mathcal{K}$ 上的代数数. 称 $\mathcal{K}(\theta)$ 为由 $\mathcal{K}$ 通过添加 θ 所得的代数扩域, m 为 θ 或 $\mathcal{K}(\theta)$ 在 $\mathcal{K}$ 上的次数. 多项式 A 在 $\mathcal{K}$ 上明显是不可约的. 我们称其为 θ 的添加多项式.

设 $F(\theta)/G(\theta)$ 为 $\mathcal{K}(\theta)$ 中的任一数. 由于 $G(\theta) \neq 0$ 且 $A \in \mathcal{K}[y]$ 在 $\mathcal{K}$ 上不可约, 所以 G 和 A 没有公共零点. 因此 $\mathrm{res}(G, A, y) \in \mathcal{K}$ 不为零. 根据引理 1.3.1, 存在多项式 $K, L \in \mathcal{K}[y]$, 使得

$$KG + LA = 1, \tag{1.4.1}$$

这里 $\deg(L, y) < \deg(G, y)$, $\deg(K, y) < \deg(A, y) = m$. 用 A 除 FK 导致如下余式公式:

$$FK = QA + R, \tag{1.4.2}$$

这里 $Q, R \in \mathcal{K}[y]$, 且 $\deg(K, y) < m$. 由表达式 (1.4.1) 和 (1.4.2) 可得

$$\frac{F}{G} = R + \left(\frac{FL}{G} - Q\right) A.$$

因 $A(\theta) = 0$, 故有

$$\frac{F(\theta)}{G(\theta)} = R(\theta).$$

因而 $\mathcal{K}(\theta)$ 中的每个数都能用一个 θ 的多项式来表示, 该多项式的次数小于或者等于 $m - 1$. 这一多项式表示是唯一的, 并可以通过代数运算构造性地确定.

注意, 上面的 θ 仅是一个符号; 一般来说, 它是不能明确给出的. 我们通常所能给出的是不可约多项式 A, 并用它来定义 θ. 鉴于这一原因, 在添加多项式 A 被提及时, 我们将简单地用 $\mathcal{K}(y)$ 来表示 $\mathcal{K}(\theta)$. 此外, 对任意 $\theta \in \mathcal{K}$ 我们约定 $\mathcal{K}(\theta) = \mathcal{K}$.

如果对每个非常数多项式 $P \in \tilde{\mathcal{K}}[x]$ 都存在 $\bar{x} \in \tilde{\mathcal{K}}$, 使得 $P(\bar{x}) = 0$, 则称域 $\tilde{\mathcal{K}} \supset \mathcal{K}$ 是代数闭的. $\mathcal{K}$ 的每个代数闭的代数扩域都称为 $\mathcal{K}$ 的一个代数闭包. 例如, 复数域 $\mathbb{C}$ 是 $\mathbb{Q}$ 的一个代数闭包.

现在考虑 $r\ (> 1)$ 个多项式构成的序列

$$A_1(y_1), A_2(y_1, y_2), \cdots, A_r(y_1, \cdots, y_r),$$

这里 $A_i \in \mathcal{K}[y_1,\cdots,y_i]$, 且 $\deg(A_i,y_i) \geq 1$ 对所有 i 成立. 这样的序列满足下面的性质: 每个 A_i —— 视作 y_i 的多项式 —— 在代数扩域 $\mathcal{K}_{i-1}$ 上不可约, 这里

$$\mathcal{K}_{i-1} = \mathcal{K}(y_1)\cdots(y_{i-1}) = \mathcal{K}(y_1,\cdots,y_{i-1}),$$

$A_1,\cdots,A_{i-1}$ 分别为 $y_1,\cdots,y_{i-1}$ 的添加多项式. 由此我们得到代数扩域序列 $\mathcal{K}_1,\cdots,\mathcal{K}_r$. 对每个 i, 由添加多项式构成的有序集合

$$\mathbb{A}_i = [A_1,\cdots,A_i]$$

称为 *不可约升列*, 而 $\mathcal{K}_i$ 则称为 $\mathcal{K}$ 以 $\mathbb{A}_i$ 为 *添加升列* 的 *代数扩域*.

设 $\mathbb{A}_r$ 以及 $\mathcal{K}_r$ 如上, 多项式 $F \in \mathcal{K}[y_1,\cdots,y_r,y]$ —— 视作 $\bar{F} \in \mathcal{K}_r[y]$ —— 在 $\mathcal{K}_r$ 上可约. 那么 $\bar{F}$ 的不可约因子分解具有以下形式:

$$\bar{F} = \bar{F}_1\cdots\bar{F}_t,$$

其中每个 $\bar{F}_i \in \mathcal{K}_r[y]$ 在 $\mathcal{K}_r$ 上不可约, 且 $t \geq 2$. 我们将在 4.3 节中看到, 存在多项式 $F_1,\cdots,F_t,Q_1,\cdots,Q_r \in \mathcal{K}[y_1,\cdots,y_r,y]$ 及 $D \in \mathcal{K}[y_1,\cdots,y_r]$, 使得

$$I\,(DF - F_1\cdots F_t) = \sum_{i=1}^{r} Q_iA_i,$$

其中 I 是 $\mathrm{lc}(A_i,y_i)$ 的幂积. 与之相应, F 在扩域 $\mathcal{K}_r$ 上的因子分解为

$$DF \doteq F_1\cdots F_t.$$

代数因子分解 问题就是从 F 和 $\mathbb{A}_r$ 构造出多项式 $F_1,\cdots,F_t$, 对此有几个算法可用. 其中两个将在 9.4 节中予以介绍.

例 1.4.1 参照例 1.1.1, 1.2.1, 1.2.3 和 1.2.4 中的多项式. 在 Q 上, F_1 和 G_3' 都是不可约的, 而 G_1,G_2,G_3,G_4' 都是可约的, 且有下面的因子分解:

$$\begin{aligned}
G_1 &= 3\,(x_4-x_3)\,(x_4-x_2+2\,x_1),\\
G_2 &= 3\,(x_4-x_3)\,(2\,x_4+5\,x_1x_2),\\
G_3 &= -9\,(x_4-x_3)\,(5\,x_1x_2+2\,x_2-4\,x_1),\\
G_4' &= -54\,x_2\,(25\,x_1^3x_2+35\,x_1^2x_2+10\,x_1x_2+4\,x_1+12)\\
&\qquad\cdot(-x_1x_3^2-x_3^2+x_1x_2x_3+x_2x_3-x_1x_2-3\,x_2).
\end{aligned}$$

令

$$\begin{aligned}
A &= 2\,x_1^2x_2^2+2\,x_1x_2^2-2\,x_1^2x_2,\\
F &= x_1x_3^2+x_3^2-x_1^2x_2x_3-x_1x_2x_3+x_1^3x_2+3\,x_1^2x_2.
\end{aligned}$$

A 和 F 在 $\mathbb{Q}$ 上都是不可约的. 在扩域 $\mathbb{Q}(x_1, x_2)$ 上 (这里 x_1 是超越元, x_2 是以 A 为添加多项式的代数元), 多项式 F 可分解如下:

$$F = (x_1 + 1)\,(x_3 - 2\,x_1x_2 + x_1)\,(x_3 + x_1x_2 - x_1).$$

1.5 零点与理想

设 $\mathcal{K}$ 是任一特征为 0 的数域, 而 $\mathcal{K}[\boldsymbol{x}]$ 是系数在 $\mathcal{K}$ 中以 $\boldsymbol{x} = (x_1, \cdots, x_n)$ 为未定元的多项式环. 又设 $\tilde{\mathcal{K}}$ 为 $\mathcal{K}$ 的任一扩域. 称 $\tilde{\mathcal{K}}$ 中的任意 n 元数组 $\bar{\boldsymbol{x}} = (\bar{x}_1, \cdots, \bar{x}_n)$ 为 $\tilde{\mathcal{K}}$ 上 n 维仿射空间 $\mathbf{A}^n$ 中的一 点. 设 $P \in \mathcal{K}[\boldsymbol{x}]$ 为一多项式. 如果 $P(\bar{\boldsymbol{x}}) = 0$, 即当 $x_1, \cdots, x_n$ 分别被 $\bar{x}_1, \cdots, \bar{x}_n$ 所替代时 P 变为零, 则称点 $\bar{\boldsymbol{x}}$ 为 P 的一个 **零点** 或者为多项式方程 $P = 0$ 的一个 **解**.

设 $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$ 为一多项式系统. 如果 $\tilde{\mathcal{K}}$ 中的一个 n 元数组是 $\mathbb{P}$ 中所有多项式的公共零点, 但不是 $\mathbb{Q}$ 中任一多项式的零点, 则称它为 $\mathfrak{P}$ 的一个 **零点**, 或者为多项式方程 $\mathbb{P} = 0$ 与不等方程 $\mathbb{Q} \neq 0$ 的一个 **解**. 我们可以考虑 $\mathfrak{P}$ 的所有零点构成的集合, 记作 $\mathrm{Zero}(\mathfrak{P})$ 或 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. 用符号表示, 即有

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) \triangleq \left\{ \bar{\boldsymbol{x}} \in \tilde{\mathcal{K}}^n : \begin{array}{l} P(\bar{\boldsymbol{x}}) = 0, Q(\bar{\boldsymbol{x}}) \neq 0, \\ \forall P \in \mathbb{P},\ Q \in \mathbb{Q} \end{array} \right\}.$$

在 $\mathbb{Q} \subset \mathcal{K} \setminus \{0\}$ 时, 我们将 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 简写为 $\mathrm{Zero}(\mathbb{P})$. 这时, $\mathrm{Zero}(\mathbb{P})$ 是 $\mathbb{P}$ 中多项式的所有公共零点构成的集合. 有时候, 我们用 $\mathrm{Zero}(\mathbb{P}/Q)$ 代替 $\mathrm{Zero}(\mathbb{P}/\{Q\})$, $\mathrm{Zero}(P/\mathbb{Q})$ 代替 $\mathrm{Zero}(\{P\}/\mathbb{Q})$ 等. 容易看出

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \mathrm{Zero}\left(\mathbb{P}/\prod_{Q\in\mathbb{Q}} Q\right) = \mathrm{Zero}(\mathbb{P}) \setminus \mathrm{Zero}\left(\prod_{Q\in\mathbb{Q}} Q\right).$$

并且对任意多项式组 $\mathbb{H}, \mathbb{P}_i, \mathbb{Q}_i$,

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_i \mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$$

蕴涵着

$$\mathrm{Zero}(\mathbb{P} \cup \mathbb{H}/\mathbb{Q}) = \bigcup_i \mathrm{Zero}(\mathbb{P}_i \cup \mathbb{H}/\mathbb{Q}_i),$$
$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q} \cup \mathbb{H}) = \bigcup_i \mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i \cup \mathbb{H}).$$

一个多项式、多项式组或多项式系统的零点的分量 $\bar{x}_i$ —— 它是 $\tilde{\mathcal{K}}$ 中的数 —— 可以仍然属于 $\mathcal{K}$. 为明确所涉及的数域 $\tilde{\mathcal{K}}$, 我们有时称上面所定义的

零点 (解) 为 $\tilde{\mathcal{K}}$ 零点 ($\tilde{\mathcal{K}}$ 解) 或 扩充零点 (扩充解). 相应地, 我们使用记号 $\tilde{\mathcal{K}}$-Zero($\mathbb{P}$), $\tilde{\mathcal{K}}$-Zero($\mathbb{P}/\mathbb{Q}$) 等.

除非另有说明, $\mathrm{Zero}(\mathfrak{P}) = \emptyset$ 总是指在基域 $\mathcal{K}$ 的 任意 扩域中, 而 $\mathrm{Zero}(\mathfrak{P}) \neq \emptyset$ 则是指在 $\mathcal{K}$ 的 某一 扩域中.

设

$$\mathbb{P} = \{P_1, \cdots, P_s\} \subset \mathcal{K}[\boldsymbol{x}]$$

为一 (非空) 多项式组. 考虑无穷多个多项式构成的集合:

$$\mathfrak{I} = \left\{ \sum_{i=1}^{s} Q_i P_i : \ Q_1, \cdots, Q_s \in \mathcal{K}[\boldsymbol{x}] \right\}.$$

定理 1.5.1 $\mathfrak{I}$ 是 $\mathcal{K}[\boldsymbol{x}]$ 中的一个 理想.

上面的理想 $\mathfrak{I}$ 称为由 $P_1, \cdots, P_s$ 或 $\mathbb{P}$ 生成的 多项式理想, 记作 Ideal($\mathbb{P}$). 我们又称 $P_1, \cdots, P_s$ 和 $\mathbb{P}$ 分别为 $\mathfrak{I}$ 的 生成元 和 生成集, 并说它们构成 $\mathfrak{I}$ 的 有限 基. 零点的定义可以自然扩展到无穷多项式组. 容易看出

$$\mathrm{Zero}(\mathrm{Ideal}(\mathbb{P})) = \mathrm{Zero}(\mathbb{P}).$$

由希尔伯特有限基定理可知, 对 $\mathcal{K}[\boldsymbol{x}]$ 的任意子集 $\mathfrak{I}$, 如果 $\mathfrak{I}$ 是理想, 则存在有限非空多项式组 $\mathbb{P}$, 使得 $\mathfrak{I} = \mathrm{Ideal}(\mathbb{P})$.

设 $\mathfrak{I}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任一理想. 无穷多项式组

$$\{F \in \mathcal{K}[\boldsymbol{x}]: \ F^m \in \mathfrak{I} \text{ 对某一整数 } m \geq 1 \text{ 成立}\}$$

构成理想, 称之为 $\mathfrak{I}$ 的 根理想, 并用 Rad($\mathfrak{I}$) 或 $\sqrt{\mathfrak{I}}$ 来表示. 也容易看出

$$\mathrm{Zero}(\sqrt{\mathfrak{I}}) = \mathrm{Zero}(\mathfrak{I}).$$

1.6 希尔伯特零点定理

多项式理想 $\mathfrak{I}$ 称为 单位理想, 如果它由常数多项式 1 生成.

定理 1.6.1 在 $\mathcal{K}$ 的任意扩域中都没有零点的多项式理想 $\mathfrak{I} \subset \mathcal{K}[\boldsymbol{x}]$ —— 即 $\mathrm{Zero}(\mathfrak{I}) = \emptyset$ —— 是单位理想.

我们可将这一定理重述如下.

定理 1.6.2 如果多项式 $P_1,\cdots,P_s \in \mathcal{K}[\boldsymbol{x}]$ 在 $\mathcal{K}$ 的某个代数闭的扩域上无公共零点，即 $\mathrm{Zero}(\{P_1,\cdots,P_s\}) = \emptyset$，则存在多项式 $Q_1,\cdots,Q_s \in \mathcal{K}[\boldsymbol{x}]$，使得下面的恒等式成立：

$$1 = Q_1P_1 + \cdots + Q_sP_s.$$

证 见 [71] 第 5 页. □

定理 1.6.2 可以看作下面希尔伯特零点定理的特殊情形.

定理 1.6.3 (零点定理) 设 $\mathbb{P} = \{P_1,\cdots,P_s\}$ 为一多项式组，而 P, P_i 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式. 如果在 $\mathcal{K}$ 的某个代数闭的扩域中有 $\mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(P)$，则存在多项式 $Q_1,\cdots,Q_s \in \mathcal{K}[\boldsymbol{x}]$，使得

$$P^q = Q_1P_1 + \cdots + Q_sP_s$$

对某一整数 $q > 0$ 成立.

关于这一定理的证明，可用著名的拉比诺维奇技巧将其化为定理 1.6.2 的情形 (见 [71] 第 6 页). 详述之：在定理的假设之下，$P_1,\cdots,P_s, Pz-1$ 无公共零点，这里 z 为一新变元. 根据定理 1.6.2，存在多项式 $H_1,\cdots,H_s,H \in \mathcal{K}[\boldsymbol{x},z]$，使得

$$1 = H_1P_1 + \cdots + H_sP_s + H\,(Pz-1).$$

在这一等式中，用 $1/P$ 替换 z 并通分. 所得分式的分子即给出定理 1.6.3 中的恒等式.

包含关系 $\mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(P)$ 意指 P 在 $P_1,\cdots,P_s$ 的所有公共零点处都为零. 有时将其写为

$$P|_{\mathrm{Zero}(\mathbb{P})} = 0. \tag{1.6.1}$$

依据定理 1.6.3 和根理想的定义，(1.6.1) 式等价于

$$P \in \sqrt{\mathrm{Ideal}(\mathbb{P})}.$$

符号 $\Longleftrightarrow$ 表示“当且仅当”. 下述定理是以上结果的一个推论.

定理 1.6.4 设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式组，而 $\mathfrak{I} = \mathrm{Ideal}(\mathbb{P})$. 那么

$$\begin{aligned} P \in \sqrt{\mathfrak{I}} &\Longleftrightarrow 1 \in \mathrm{Ideal}(\mathbb{P} \cup \{Pz-1\}) \\ &\Longleftrightarrow \mathrm{Zero}(\mathbb{P} \cup \{Pz-1\}) = \emptyset, \end{aligned}$$

其中 z 为一新变元.

第二章　多项式系统的零点分解

从这一章开始，我们进入本书的主题 —— 描述将任意多元多项式系统分解为特殊的三角形系统的消去算法. 同时将建立给定系统与所得系统之间的各种零点关系. 本章介绍三种互异而又相关的算法，用以计算弱形式的零点分解.

2.1 三角系统

设 $\mathcal{K}$ 是一特征为 0 的可计算数域. 有理数域 Q 是 $\mathcal{K}$ 的一个实例. 多项式组即是 $\mathcal{K}[\boldsymbol{x}]$ 中非零多项式构成的有限基合. 凡说到 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统，我们是指一对多项式组 $[\mathbb{P},\mathbb{Q}]$，其零点集 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 是我们的兴趣所在. 换言之，我们所关心的是多项式方程 $\mathbb{P}=0$ 与不等方程 $\mathbb{Q}\neq 0$ 的解.

本书中，有限集合 $\mathbb{S}$ 中元素的个数用 $|\mathbb{S}|$ 来表示. 它也称为 $\mathbb{S}$ 的 *长度*. 关于 *有序集合* 的表达，我们将其元素列入一对方括号中. 对任一非空有序集合

$$\mathbb{T}=[T_1,T_2,\cdots,T_r]$$

和整数 $1\le i\le r$，下面的记号经常用到:

$$\mathrm{op}(i,\mathbb{T})\triangleq T_i,\quad \mathbb{T}^{\{i\}}\triangleq[T_1,\cdots,T_i].$$

设 $\mathbb{S}=[S_1,\cdots,S_s]$ 为另一与 $\mathbb{T}$ 无交的有序集. 我们定义

$$\mathbb{S}\cup\mathbb{T}\triangleq[S_1,\cdots,S_s,T_1,\cdots,T_r].$$

$\mathbb{S}\cup\mathbb{T}$ 和 $\mathbb{T}\cup\mathbb{S}$ 作为有序集是有区别的. 换言之，在对无交有序集合求并时，其元素的次序保持不变. 如果 $\mathbb{S}$ 和 $\mathbb{T}$ 二者或之一是通常的 (无序) 集合，那么 $\mathbb{S}\cup\mathbb{T}=\mathbb{T}\cup\mathbb{S}$ 也是.

定义 2.1.1　$\mathcal{K}[\boldsymbol{x}]$ 中非常数多项式组成的有限非空有序集合

$$\mathbb{T}=[T_1,T_2,\cdots,T_r]$$

称为 *三角列* 或 *非矛盾拟升列*，如果

$$\mathrm{cls}(T_1)<\mathrm{cls}(T_2)<\cdots<\mathrm{cls}(T_r).$$

可将任意三角列写成如下形式:

$$\mathbb{T}=\begin{bmatrix} T_1(x_1,\cdots,x_{p_1}), \\ T_2(x_1,\cdots,x_{p_1},\cdots,x_{p_2}), \\ \cdots\cdots\cdots\cdots \\ T_r(x_1,\cdots,x_{p_1},\cdots,x_{p_2},\cdots,x_{p_r}) \end{bmatrix}, \tag{2.1.1}$$

这里

$$0<p_1<p_2<\cdots<p_r\le n,$$
$$p_i=\mathrm{cls}(T_i),\ x_{p_i}=\mathrm{lv}(T_i),\quad i=1,\cdots,r.$$

设 $\mathbb{T}$ 为 (2.1.1) 所示的三角列, 而 P 为任一多项式. 如果 P 对每个 $T\in\mathbb{T}$ 都是约化的, 即 $\deg(P,x_{p_i})<\mathrm{ldeg}(T_i)$ 对所有 i 成立, 则称 P 对 $\mathbb{T}$ *是约化的*. 将多项式

$$R=\mathrm{prem}(\cdots\mathrm{prem}(P,T_r),\cdots,T_1)$$

简记为 $\mathrm{prem}(P,\mathbb{T})$, 并称其为 P 对 $\mathbb{T}$ 的 *伪余式*. 由表达式 (1.2.1) 容易导出下面的 *伪余公式*:

$$I_1^{q_1}\cdots I_r^{q_r}P=\sum_{i=1}^{r}Q_iT_i+R, \tag{2.1.2}$$

这里 q_i 是非负整数, 而

$$I_i=\mathrm{ini}(T_i),\ Q_i\in\mathcal{K}[\boldsymbol{x}],\quad i=1,\cdots,r.$$

明显地, 在 P 对 $\mathbb{T}$ 是约化的情形有 $\mathrm{prem}(P,\mathbb{T})=P$. 对任意多项式组 $\mathbb{P}$, $\mathrm{prem}(\mathbb{P},\mathbb{T})$ 代表 $\{\mathrm{prem}(P,\mathbb{T}):\ P\in\mathbb{P}\}$.

例 2.1.1 考虑例 1.1.2 中的多项式 F_1,F_2, 且命

$$F_3=x_3x_4-2\,x_2^2-x_1x_2-1,$$
$$F_4=\mathrm{prem}(F_1,F_2).$$

F_4 的计算已在例 1.2.3 中给出. F_3 对 F_1 是约化的, 但 F_1 对 F_3 是非约化的. 而且 F_2 与 F_3 二者中没有一个对另一个是约化的. 关于 $x_1\prec\cdots\prec x_4$, $\mathbb{T}_1=[F_4,F_2]$ 是三角列. F_1 和 F_3 对 $\mathbb{T}_1$ 都不是约化的. 可以验算

$$F_6=\mathrm{prem}(F_3,\mathbb{T}_1)=2\,x_1x_2^2+2\,x_1^2x_2^2-2\,x_1^2x_2+x_1^2+x_1,$$
$$\mathrm{prem}(F_1,\mathbb{T}_1)=0.$$

在下面的定义中以及其他地方，对有序集合求差时元素的次序将按照自然的方式保持不变. 例如，$[a,b,c,d]\setminus[a,c]=[b,d]$.

定义 2.1.2 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{T},\mathbb{U}]$ 称为 *三角系统*, 如果 $\mathbb{T}$ 是三角列，且对任意类为 i 的 $I\in \mathrm{ini}(\mathbb{T})$ 以及 $\bar{\boldsymbol{x}}\in \mathrm{Zero}(\mathbb{T}^{(i)}/\mathbb{U})$ 都有 $I(\bar{\boldsymbol{x}})\neq 0$.

如果 $0\notin \mathrm{prem}(\mathbb{U},\mathbb{T})$, 则称三角系统 $[\mathbb{T},\mathbb{U}]$ 为 *良好的*. 如果每个 $T\in\mathbb{T}\cup\mathbb{U}$ 对 $\mathbb{T}\setminus[T]$ 都是约化的，则称 $[\mathbb{T},\mathbb{U}]$ 是 *约化的*.

引理 2.1.1 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意三角系统 $[\mathbb{T},\mathbb{U}]$ 与多项式 P, 如果 $\mathrm{prem}(P,\mathbb{T})=0$, 则 $\mathrm{Zero}(\mathbb{T}/\mathbb{U})\subset \mathrm{Zero}(P)$.

证 设 $\bar{\boldsymbol{x}}\in \mathrm{Zero}(\mathbb{T}/\mathbb{U})$. 根据定义，对任意 $I\in \mathrm{ini}(\mathbb{T})$ 有 $I(\bar{\boldsymbol{x}})\neq 0$. 因此由伪余公式 (2.1.2) 可得 $P(\bar{\boldsymbol{x}})=0$. □

定义 2.1.3 称三角列 $\mathbb{T}\subset\mathcal{K}[\boldsymbol{x}]$ 分别为 *良好的* 或者 *约化的*, 如果 $[\mathbb{T},\mathrm{ini}(\mathbb{T})]$ 是良好的或者约化的.

约化的三角列也被称作 *非矛盾升列*.

三角列 $\mathbb{T}$ 称为 *非矛盾弱升列*, 如果对每个 $T\in\mathbb{T}$, $\mathrm{ini}(T)$ 对 $\mathbb{T}\setminus[T]$ 都是约化的.

又称任意单个非零常数构成的集合为 *矛盾 (拟 、 弱) 升列*.

注意：任意多项式对一矛盾升列的伪余式为 0.

例 2.1.2 置 $x_1\prec x_2\prec x_3$ 及 $\mathbb{T}=[x_1-2,(x_1^2-4)\,x_3+x_2]$. $\mathbb{T}$ 是三角列，但不是良好的. $[\mathbb{T},\{x_1,x_1-2\}]$ 是 (非良好的) 三角系统，而 $[\mathbb{T},\{x_1+2\}]$ 不是三角系统. 三角列

$$[x_1^2-2,x_2^2-2\,x_1x_2+2,(x_2-x_1)\,x_3+1]$$

既是良好的又是约化的，因而是非矛盾升列.

容易证明, 如果 $[\mathbb{T},\mathbb{U}]$ 是良好三角系统, 则或者 $\mathbb{T}$ 是良好的, 或者 $\mathrm{Zero}(\mathbb{T}/\mathbb{U})=\emptyset$.

引理 2.1.2 设 $F\in\mathcal{K}[x]$, $G\in\mathcal{K}[x,y]$ 为多项式，则

$$\mathrm{prem}(\mathrm{coef}(G,y^k),F,x)\neq 0 \iff \mathrm{coef}(\mathrm{prem}(G,F,x),y^k)\neq 0 \qquad (2.1.3)$$

对任意 $0\leq k\leq \deg(G,y)$ 成立.

证 命 $I = \mathrm{lc}(F, x), m = \deg(F, x), l = \deg(G, y)$, 并将 G 写成

$$G = G_l y^l + G_{l-1} y^{l-1} + \cdots + G_0, \quad G_i \in \mathcal{K}[x].$$

又令

$$R_i = \mathrm{prem}(G_i, F, x), \quad i = 0, 1, \cdots, l.$$

相应于伪余公式 (1.2.1), 我们有

$$I^{q_i} G_i = Q_i F + R_i, \quad q_i = \max(\deg(G_i, x) - m + 1, 0) \tag{2.1.4}$$

对任意 i 成立. 令

$$q = \max(\deg(G, x) - m + 1, 0) = \max_{0 \le i \le l} q_i.$$

对每个 i 将 (2.1.4) 中的伪余公式乘以 $y^i I^{q-q_i}$, 并将所得的公式全部相加, 我们有

$$I^q G = (\sum_{i=0}^{l} I^{q-q_i} Q_i y^i) F + \sum_{i=0}^{l} I^{q-q_i} R_i y^i.$$

由命题 1.2.2 得

$$\sum_{i=0}^{l} I^{q-q_i} R_i y^i = \mathrm{prem}(G, F, x).$$

因而

$$\mathrm{coef}(\mathrm{prem}(G, F, x), y^k) = I^{q-q_k} R_k = I^{q-q_k} \mathrm{prem}(\mathrm{coef}(G, y^k), F, x)$$

对任意 $0 \le k \le l$ 成立. 显而易见, $I \ne 0$; 由此 (2.1.3) 获证. □

以下结果是引理 2.1.2 的一个明显推论.

推论 2.1.3 设 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 为三角列, 而 $P \in \mathcal{K}[\boldsymbol{x}, y]$ 为任意多项式, 这里 y 是新变元. 那么

$$\mathrm{prem}(\mathrm{coef}(P, y^k), \mathbb{T}) \ne 0 \iff \mathrm{coef}(\mathrm{prem}(P, \mathbb{T}), y^k) \ne 0$$

对任意 $0 \le k \le \deg(P, y)$ 成立.

引理 2.1.4 从任意良好三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 可求得一约化三角列 $\mathbb{T}^*$, 使得

$$\mathrm{Zero}(\mathbb{T}^* / \mathrm{ini}(\mathbb{T}^*)) = \mathrm{Zero}(\mathbb{T} / \mathrm{ini}(\mathbb{T})). \tag{2.1.5}$$

证 命 $\mathbb{T}=[T_1,\cdots,T_r]$, 且

$$p_i=\mathrm{cls}(T_i),\ I_i=\mathrm{ini}(T_i),\quad i=1,\cdots,r.$$

因 $r=1$ 为平凡情形, 故可假定 $r>1$, 并令

$$\begin{aligned}\mathbb{T}^{\{i-1\}}&=[T_1,\cdots,T_{i-1}],\\ T_i^*&=\mathrm{prem}(T_i,\mathbb{T}^{\{i-1\}}),\\ \mathbb{T}^{*\{i\}}&=[T_1,T_2^*,\cdots,T_i^*],\quad i=2,\cdots,r.\end{aligned}$$

由于 $\mathbb{T}^{\{i-1\}}$ 不含有变元 $x_{p_i},\cdots,x_n$, 依推论 2.1.3 有

$$\mathrm{cls}(T_i^*)=p_i,\ \mathrm{ldeg}(T_i^*)=\mathrm{ldeg}(T_i),\quad 2\le i\le r.$$

所以 $\mathbb{T}^*$ 是一约化三角列.

为了证明 (2.1.5), 我们写出与 (2.1.2) 相应的伪余公式如下:

$$T_i^*=I_1^{q_{i1}}\cdots I_{i-1}^{q_{i,i-1}}T_i+\sum_{j=1}^{i-1}Q_{ij}T_j,\quad 2\le i\le r. \tag{2.1.6}$$

设 $\bar{\boldsymbol{x}}_{p_{i-1}}\in\mathrm{Zero}(\mathbb{T}^{\{i-1\}}/\mathrm{ini}(\mathbb{T}^{\{i-1\}}))$. 由 (2.1.6) 可知

$$\bar{T}_i^*=I_1^{q_{i1}}(\bar{\boldsymbol{x}}_{p_{i-1}})\cdots I_{i-1}^{q_{i,i-1}}(\bar{\boldsymbol{x}}_{p_{i-1}})\bar{T}_i,$$

其中

$$\begin{aligned}\bar{T}_i&=T_i(\bar{\boldsymbol{x}}_{p_{i-1}},x_{p_{i-1}+1},\cdots,x_{p_i}),\\ \bar{T}_i^*&=T_i^*(\bar{\boldsymbol{x}}_{p_{i-1}},x_{p_{i-1}+1},\cdots,x_{p_i}).\end{aligned}$$

因此 $\bar{T}_i^*$ 和 $\bar{T}_i$ 对 $x_{p_{i-1}+1},\cdots,x_{p_i}$ 具有相同的零点集. 由于这一结论对任意 $i\ge 2$ 成立, 故有

$$\mathrm{Zero}(\bar{T}_i^*/\mathrm{ini}(\bar{T}_i^*))=\mathrm{Zero}(\bar{T}_i/\mathrm{ini}(\bar{T}_i));$$

于是

$$\mathrm{Zero}(\mathbb{T}^{*\{i\}}/\mathrm{ini}(\mathbb{T}^{*\{i\}}))=\mathrm{Zero}(\mathbb{T}^{\{i\}}/\mathrm{ini}(\mathbb{T}^{\{i\}})).$$

在 $i=r$ 时即得 (2.1.5). □

注 2.1.1　设 $[\mathbb{T},\mathbb{U}]$ 为良好三角系统, 且 $\text{Zero}(\mathbb{T}/\mathbb{U}) \neq \emptyset$. 这时 $\mathbb{T}$ 也是良好的. 因此, 我们可求得一约化三角列 $\mathbb{T}^*$ 使得 (2.1.5) 成立. 置 $\mathbb{U}^* = \text{prem}(\mathbb{U},\mathbb{T}^*)$, 则

$$\begin{aligned}\text{Zero}(\mathbb{T}^*/\mathbb{U}^*) &= \text{Zero}(\mathbb{T}^*/\text{ini}(\mathbb{T}^*)\cup\mathbb{U}^*)\\ &= \text{Zero}(\mathbb{T}/\text{ini}(\mathbb{T})\cup\mathbb{U}) = \text{Zero}(\mathbb{T}/\mathbb{U}).\end{aligned}$$

也就是说, 可从 $[\mathbb{T},\mathbb{U}]$ 求得一约化三角系统 $[\mathbb{T}^*,\mathbb{U}^*]$, 使得

$$\text{Zero}(\mathbb{T}^*/\mathbb{U}^*) = \text{Zero}(\mathbb{T}/\mathbb{U}).$$

本章的主要目的在于给出算法, 用以将任给多项式系统 $\mathfrak{P}$ 分解为有限多个良好三角系统 $\mathfrak{T}_1,\cdots,\mathfrak{T}_e$, 使得

$$\text{Zero}(\mathfrak{P}) = \bigcup_{i=1}^{e}\text{Zero}(\mathfrak{T}_i) \tag{2.1.7}$$

成立. 在 $\text{Zero}(\mathfrak{P}) = \emptyset$ 得到确认时, 我们置 $e = 0$.

2.2 基于特征列的算法

特征列的概念是里特[61, 62]在其有关微分代数的工作中对 (微分) 多项式理想引进的. 然而, 在 1978 年吴文俊意识到他所创立的几何定理机器证明方法的构造性代数工具的基础已见诸于里特的两本著作之前, 里特所提出的概念和方法并未引起人们的注意. 从那时起, 吴通过删除里特运用连续性和极限等概念的解析论证, 修正其概念与方法以适用于多项式组而非理想, 以及通过各种几何应用来说明其高效率和实用性而极大地发展了里特的工作. 譬如说, 吴丢弃了里特算法中的一个主要限制 —— *不可约性*, 因而使得我们可以有效地从任意多项式组构造出特征列来. 吴的洞察力和大量工作大大激发了人们对该学科的兴趣与研究. 所有这些都对特征列方法的理论发展作出了重要贡献, 并使其对实际应用更加合适有效. 本书中介绍的基于特征列的算法大多属于吴的工作[95, 97, 100, 101, 96]

里特 – 吴特征列

定义 2.2.1　称 $K[\boldsymbol{x}]$ 中的非零多项式 F 比 G 有 *较低的秩*, 记作 $F \prec G$ 或 $G \succ F$, 如果 $\text{cls}(F) < \text{cls}(G)$, 或者 $\text{cls}(F) = \text{cls}(G) > 0$, 且 $\text{ldeg}(F) < \text{ldeg}(G)$. 这时, 也称 G 比 F 有 *较高的秩*.

如果 $F \prec G$ 和 $G \prec F$ 都不成立, 则称 F 和 G 具有 *相同的秩*, 记作 $F \sim G$.

我们将 "$F \prec G$ 或 $F \sim G$" 写成 $F \precsim G$. 类似地有 "$\succsim$".

例 2.2.1 考虑例 1.1.2 和 2.1.1 中的多项式 F_1, F_2, F_3. 对 $x_1 \prec \cdots \prec x_4$, 我们有

$$\begin{aligned}
&\mathrm{cls}(F_1) = \mathrm{cls}(F_2) = \mathrm{cls}(F_3) = 4, \\
&\mathrm{ldeg}(F_1) = 2, \quad \mathrm{ldeg}(F_2) = \mathrm{ldeg}(F_3) = 1.
\end{aligned}$$

由此可知 $F_3 \sim F_2$, $F_2 \prec F_1$.

定义 2.2.2 对任意三角列

$$\mathbb{T} = [T_1, \cdots, T_r], \quad \mathbb{T}' = [T_1', \cdots, T_{r'}'],$$

如果存在 $j \le \min(r, r')$, 使得

$$T_1 \sim T_1', \cdots, T_{j-1} \sim T_{j-1}', \quad 而 \quad T_j \succ T_j';$$

或者 $r' > r$, 且 $T_1 \sim T_1', \cdots, T_r \sim T_r'$, 则称 $\mathbb{T}$ 比 $\mathbb{T}'$ 有 *较高的秩*, 记作 $\mathbb{T} \succ \mathbb{T}'$ 或 $\mathbb{T}' \prec \mathbb{T}$. 此时, 也称 $\mathbb{T}'$ 比 $\mathbb{T}$ 有 *较低的秩*. 如果 $\mathbb{T} \prec \mathbb{T}'$ 和 $\mathbb{T}' \prec \mathbb{T}$ 都不成立, 则称 $\mathbb{T}$ 和 $\mathbb{T}'$ 具有 *相同的秩*, 记作 $\mathbb{T} \sim \mathbb{T}'$. 这时有

$$r = r', \quad 且 \quad T_1 \sim T_1', \cdots, T_r \sim T_r'.$$

例 2.2.2 设多项式 $F_1, \cdots, F_4$ 如例 1.1.2 和 2.1.1 中所示, 且命

$$F_5 = \mathrm{prem}(F_3, F_2) = -x_3^2 + x_1x_2x_3 - 2\,x_1x_2^2 - x_1^2x_2 - x_1,$$

则

$$\mathbb{T}_1 = [F_4, F_2], \quad \mathbb{T}_2 = [F_5, F_2], \quad \mathbb{T}_3 = [F_4, F_1]$$

均为约化三角列. $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 具有相同的秩, 该秩比 $\mathbb{T}_3$ 的秩低, 即 $\mathbb{T}_1 \sim \mathbb{T}_2 \prec \mathbb{T}_3$.

以上定义的 "$\precsim$" 为半序, 在其之下可将所有三角列排序. 因此, 对升列组成的集合, 我们可以谈论其 *极小升列* 的概念, 如果该升列存在.

引理 2.2.1 设 $\mathbb{T}_1 \succsim \mathbb{T}_2 \succsim \cdots \succsim \mathbb{T}_k \succsim \cdots$ 为一串三角列, 其秩永不递增, 则存在整数 k', 使得 $\mathbb{T}_k \sim \mathbb{T}_{k'}$ 对所有 $k \ge k'$ 成立.

证 对每个 k, 命 $T_k = \mathrm{op}(1, \mathbb{T}_k)$, $r_k = |\mathbb{T}_k|$ (记住: $\mathrm{op}(i, \mathbb{T}_k)$ 表示 $\mathbb{T}_k$ 的第 i 个元素). 于是

$$T_1 \succsim T_2 \succsim \cdots \succsim T_k \succsim \cdots.$$

换言之, 对任意 k, 或者 $\mathrm{cls}(T_{k+1}) < \mathrm{cls}(T_k)$, 或者

$$\mathrm{cls}(T_{k+1}) = \mathrm{cls}(T_k) > 0 \text{ 且 } \mathrm{ldeg}(T_{k+1}) \le \mathrm{ldeg}(T_k).$$

由于类和次数都是非负整数, 故存在下标 k_1, 使得 $T_k \sim T_{k_1}$ 对所有 $k \ge k_1$ 成立.

如果存在 $k_1' \ge k_1$, 使得对所有 $k \ge k_1'$ 有 $r_k = 1$, 那么引理明显成立. 否则, 存在 $k_1' \ge k_1$, 使得 $r_k \ge 2$ 对所有 $k \ge k_1'$ 成立. 对 $k \ge k_1'$, 命 $T_k' = \mathrm{op}(2, \mathbb{T}_k)$, 则有

$$T_{k_1'}' \succsim T_{k_1'+1}' \succsim \cdots \succsim T_k' \succsim \cdots.$$

因此和前面一样, 存在 $k_2 \ge k_1'$, 使得 $T_k' \sim T_{k_2}'$ 对所有 $k \ge k_2$ 成立.

如果对所有 $k \ge k_2$ 有 $r_k \le 2$, 那么引理已被证明. 否则, 存在 $k_2' \ge k_2$, 使得 $r_k \ge 3$ 对所有 $k \ge k_2'$ 成立. 这时, 我们可以考虑 $T_k'' = \mathrm{op}(3, \mathbb{T}_k)$, 并构造一秩非递增的多项式序列. 由于对所有 k 都有 $r_k \le n$, 按这种方式继续下去我们必定停止于某个 r 与 k', 使得

$$r_k = r, \ \mathrm{op}(r, \mathbb{T}_k) \sim \mathrm{op}(r, \mathbb{T}_{k'}), \quad \forall k \ge k'.$$

因而 $\mathbb{T}_k \sim \mathbb{T}_{k'}$ 对所有 $k \ge k'$ 成立. 引理获证. □

考虑任意非空多项式组 $\mathbb{P}$. 设 Φ 为所有包含于 $\mathbb{P}$ 的升列构成的集合. 由于每个单个多项式都构成升列, 所以 $\Phi \ne \emptyset$. 称 Φ 的任意极小升列为 $\mathbb{P}$ 的**基列**. 这样的基列存在, 并可按如下步骤确定.

从 $\mathbb{P} = \mathbb{F}_1$ 开始, 我们在其中选取一个秩最低的多项式, 譬如说 B_1. 若 $\mathrm{cls}(B_1) = 0$, 则 $[B_1]$ 是 $\mathbb{P}$ 的一基列. 否则, 命

$$\mathbb{F}_2 = \{F \in \mathbb{F}_1 \setminus \{B_1\}: \ F \text{ 对 } B_1 \text{ 是约化的}\}.$$

如果 $\mathbb{F}_2 = \emptyset$, 那么 $[B_1]$ 是 $\mathbb{F}_1 = \mathbb{P}$ 的一基列. 由 B_1 的选取可知, $\mathbb{F}_2$ 中的所有多项式都比 B_1 有较高的秩. 现设 B_2 为 $\mathbb{F}_2$ 中秩最低的多项式, 且命

$$\mathbb{F}_3 = \{F \in \mathbb{F}_2 \setminus \{B_2\}: \ F \text{ 对 } B_2 \text{ 是约化的}\}.$$

若 $\mathbb{F}_3=\emptyset$, 则 $[B_1,B_2]$ 为 $\mathbb{P}$ 的一基列. 否则, 从 $\mathbb{F}_3$ 中选取一秩最低的多项式 B_3, 并按上述方式继续进行. 由于

$$\mathrm{cls}(B_1)<\mathrm{cls}(B_2)<\mathrm{cls}(B_3)<\cdots\leq n,$$

这一程序必定在有限步内停止, 而最终获得 $\mathbb{P}$ 的一基列.

下面的算法更确切地给出了上述选择过程.

算法 BasSet: $\mathbb{B}\leftarrow\mathrm{BasSet}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P}\subset\mathcal{K}[\boldsymbol{x}]$, 本算法计算 $\mathbb{P}$ 的基列 $\mathbb{B}$.

B1. 命 $\mathbb{F}\leftarrow\mathbb{P}$, $\mathbb{B}\leftarrow\emptyset$.

B2. 重复下列步骤直至 $\mathbb{F}=\emptyset$:

B2.1. 从 $\mathbb{F}$ 中选取一秩最低的多项式 B.

B2.2. 命 $\mathbb{B}\leftarrow\mathbb{B}\cup[B]$.

B2.3. 如果 $\mathrm{cls}(B)=0$, 则命 $\mathbb{F}\leftarrow\emptyset$; 否则命

$$\mathbb{F}\leftarrow\{F\in\mathbb{F}\setminus\{B\}:\ F \text{ 对 } B \text{ 是约化的}\}.$$

$\mathbb{P}$ 的某一基列是矛盾的当且仅当 $\mathbb{P}$ 含有常数. 在这一情形, 算法 BasSet 终止于 B2 的第一个循环. 关于基列的例子, 参阅例 2.2.3.

定义 2.2.3 称升列 $\mathbb{C}$ 为非空多项式组 $\mathbb{P}\subset\mathcal{K}[\boldsymbol{x}]$ 的 *特征列*, 如果

$$\mathbb{C}\subset\mathrm{Ideal}(\mathbb{P}),\quad \mathrm{prem}(\mathbb{P},\mathbb{C})=\{0\}.$$

这里, $\mathbb{P}$ 的特征列是按照吴的方式定义的. 里特关于特征列的定义是对 ($\mathbb{P}$ 生成的) 理想 $\mathfrak{I}$ 而言, 而且要求 $\mathrm{prem}(\mathfrak{I},\mathbb{C})=\{0\}$; 因此, 为了计算 $\mathbb{C}$, 人们不得不像 4.3 节中那样考虑它的 *不可约性*, 或者使用其他算法 (参阅 [57] 中 5.6 节).

命题 2.2.2 设 $\mathbb{C}=[C_1,\cdots,C_r]$ 为多项式组 $\mathbb{P}\subset\mathcal{K}[\boldsymbol{x}]$ 的特征列, 且命

$$\begin{aligned}&I_i=\mathrm{ini}(C_i),\ \mathbb{P}_i=\mathbb{P}\cup\{I_i\},\quad i=1,\cdots,r,\\&\mathbb{I}=\mathrm{ini}(\mathbb{C})=\{I_1,\cdots,I_r\},\end{aligned}$$

则

$$\mathrm{Zero}(\mathbb{C}/\mathbb{I}) \subset \mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(\mathbb{C}), \tag{2.2.1}$$

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{C}/\mathbb{I}) \cup \bigcup_{i=1}^{r} \mathrm{Zero}(\mathbb{P}_i) \tag{2.2.2}$$

在 $\mathcal{K}$ 以及 $\mathcal{K}$ 的任意扩域中成立.

证　因 $\mathbb{C} \subset \mathrm{Ideal}(\mathbb{P})$, 故 $\mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(\mathbb{C})$.

另一方面，对任意 $P \in \mathbb{P}$ 都存在非负整数 q_i 与多项式 Q_i, 使得

$$I_1^{q_1} \cdots I_r^{q_r} P = \sum_{i=1}^{r} Q_i C_i.$$

由此可见 $\mathrm{Zero}(\mathbb{C}/\mathbb{I}) \subset \mathrm{Zero}(\mathbb{P})$. 很明显，这一关系对 $\mathcal{K}$ 及 $\mathcal{K}$ 的任意扩域都成立. 因而 (2.2.1) 获证.

注意： $\mathbb{P}$ 和 I_i 的公共零点即是 $\mathbb{P}_i$ 的零点. 因此容易得出关系式 (2.2.2). □

现在, 我们可以着手描述里特 - 吴的特征列算法 —— 该算法指出如何从任意多项式组求得其特征列.

算法 CharSet: $\mathbb{C} \leftarrow \mathrm{CharSet}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算 $\mathbb{P}$ 的特征列 $\mathbb{C}$.

C1. 命 $\mathbb{F} \leftarrow \mathbb{P}$, $\mathbb{R} \leftarrow \mathbb{P}$.

C2. 重复下列步骤直至 $\mathbb{R} = \emptyset$:

C2.1. 计算 $\mathbb{C} \leftarrow \mathrm{BasSet}(\mathbb{F})$.

C2.2. 如果 $\mathbb{C}$ 是矛盾列，则命 $\mathbb{R} \leftarrow \emptyset$; 否则计算

$$\mathbb{R} \leftarrow \mathrm{prem}(\mathbb{F} \setminus \mathbb{C}, \mathbb{C}) \setminus \{0\},$$

且命 $\mathbb{F} \leftarrow \mathbb{F} \cup \mathbb{R}$.

特征列算法是零点分解算法 CharSer, IrrCharSer 和 IrrCharSerE 的核心，并有诸多应用. 为了证明这一算法的终止性，我们先来证明下述引理.

引理 2.2.3 设 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 是以

$$\mathbb{B} = [B_1, B_2, \cdots, B_r]$$

为基列的非空多项式组，这里 $\text{cls}(B_1) > 0$. 如果 B 是一对 $\mathbb{B}$ 约化的非零多项式，那么 $\mathbb{P} \cup \{B\}$ 有一基列，其秩比 $\mathbb{B}$ 的秩低.

证 命 $\mathbb{P}^+ = \mathbb{P} \cup \{B\}$. 若 $\text{cls}(B) = 0$, 则 $[B]$ 是 $\mathbb{P}^+$ 的基列，并且比 $\mathbb{B}$ 有较低的秩. 不然的话，假定 $\text{cls}(B) = p > 0$. 因 B 对 $\mathbb{B}$ 是约化的，故存在 i $(1 \le i \le r)$, 使得 $p \le \text{cls}(B_i)$, 且在 $i > 1$ 时有 $p > \text{cls}(B_{i-1})$. 而且在 $p = \text{cls}(B_i)$ 时有 $\deg(B, x_p) < \text{ldeg}(B_i)$. 于是

$$[B_1, B_2, \cdots, B_{i-1}, B]$$

是包含于 $\mathbb{P}^+$ 的升列，并且比 $\mathbb{B}$ 有较低的秩. 因而 $\mathbb{P}^+$ 的基列比 $\mathbb{B}$ 有较低的秩. □

CharSet 的证明 可将算法 CharSet 图示如下：

$$\begin{array}{cccccccccc} \mathbb{P} = & \mathbb{F}_1 & \subset & \mathbb{F}_2 & \subset & \cdots & \subset & \mathbb{F}_m & & \\ & \cup & & \cup & & & & \cup & & \\ & \mathbb{B}_1 & & \mathbb{B}_2 & & \cdots & & \mathbb{B}_m & = & \mathbb{C} \\ & \mathbb{R}_1 & & \mathbb{R}_2 & & \cdots & & \mathbb{R}_m & = & \emptyset \end{array} \tag{2.2.3}$$

其中

$$\mathbb{R}_i = \text{prem}(\mathbb{F}_i \setminus \mathbb{B}_i, \mathbb{B}_i) \setminus \{0\},$$
$$\mathbb{F}_{i+1} = \mathbb{F}_i \cup \mathbb{R}_i,$$

且 $\mathbb{B}_i$ 是 $\mathbb{F}_i$ 的基列.

终止性. 我们需要证明步骤 C2 仅有有限多个循环，即 (2.2.3) 中的 m 是有限的. 如果某一 $\mathbb{B}_i$ 是矛盾列，则算法显然终止. 否则，依引理 2.2.3, 对所有 i 有 $\mathbb{B}_{i+1} \prec \mathbb{B}_i$. 于是 $\mathbb{B}_1 \succ \mathbb{B}_2 \succ \cdots$. 由引理 2.2.1 知，该序列至多有有限项构成. 换言之， m 是有限的，因而算法 CharSet 必须终止.

正确性. 由 (2.1.2) 式知, 对任意多项式 $F \in \mathbb{F}_i$ 有 $\text{prem}(F, \mathbb{B}_i) \in \text{Ideal}(\mathbb{B}_i \cup \{F\})$. 因而

$$\text{Ideal}(\mathbb{F}_{i+1}) = \text{Ideal}(\mathbb{F}_i) = \text{Ideal}(\mathbb{P})$$

对所有 i 成立. 于是

$$\mathbb{C} = \mathbb{B}_m \subset \mathbb{F}_m \subset \text{Ideal}(\mathbb{P}).$$

由于 $\mathbb{R}_m = \emptyset$, 我们有

$$\operatorname{prem}(\mathbb{F}_m, \mathbb{C}) = \operatorname{prem}(\mathbb{F}_m \setminus \mathbb{C}, \mathbb{C}) \cup \operatorname{prem}(\mathbb{C}, \mathbb{C}) = \{0\}.$$

根据定义, $\mathbb{C}$ 是 $\mathbb{P}$ 的特征列. 证毕. □

上述由 $\mathbb{P}$ 获取特征列 $\mathbb{C}$ 的过程被吴[95, 97]称之为*整序原理*, 并被归功于里特.

例 2.2.3 命 $\mathbb{P} = \{F_1, F_2, F_3\}$, 其中

$$\begin{aligned}
F_1 &= x_1x_4^2 + x_4^2 - x_1x_2x_4 - x_2x_4 + x_1x_2 + 3\,x_2, \\
F_2 &= x_1x_4 + x_3 - x_1x_2, \\
F_3 &= x_3x_4 - 2\,x_2^2 - x_1x_2 - 1.
\end{aligned}$$

这些多项式已在例 1.1.2 和 2.1.1 中出现. 对应于图 (2.2.3) 中的多项式组及其基列如下:

$$\begin{array}{llll}
\mathbb{P} = & \mathbb{F}_1 = \{F_1, F_2, F_3\} \quad \subset & \mathbb{F}_2 = \{F_1, \cdots, F_5\} \quad \subset & \mathbb{F}_3 = \{F_1, \cdots, F_6\} \\
& \cup & \cup & \cup \\
& \mathbb{B}_1 = [F_2] & \mathbb{B}_2 = [F_4, F_2] & \mathbb{B}_3 = [F_6, F_4, F_2] = \mathbb{C} \\
& \mathbb{R}_1 = \{F_4, F_5\} & \mathbb{R}_2 = \{F_6\} & \mathbb{R}_3 = \emptyset,
\end{array}$$

其中 F_4, F_5, F_6 已在例 2.1.1 和 2.2.2 中给出. 所以, 最后一个基列 $\mathbb{B}_3$ 即是 $\mathbb{P}$ 的特征列 $\mathbb{C}$. 将多项式 F_6, F_4, F_2 重新命名为 C_1, C_2, C_3, 并抄录如下以备参考:

$$\begin{aligned}
\mathbb{C} &= [C_1, C_2, C_3] \\
&= \begin{bmatrix}
x_1\,(2\,x_1x_2^2 + 2\,x_2^2 - 2\,x_1x_2 + x_1 + 1), \\
x_1x_3^2 + x_3^2 - x_1^2x_2x_3 - x_1x_2x_3 + x_1^3x_2 + 3\,x_1^2x_2, \\
x_1x_4 + x_3 - x_1x_2
\end{bmatrix}.
\end{aligned}$$

C_1, C_2, C_3 的初式分别为

$$I_1 = 2\,x_1\,(x_1 + 1), \quad I_2 = x_1 + 1, \quad I_3 = x_1.$$

由于 I_2 和 I_3 都是 I_1 的因子, $I_1 \neq 0$ 意味着 $I_1I_2I_3 \neq 0$. 于是只有初式 I_1 需要进一步考虑. 设 $\mathbb{P}_1$ 与 $\mathbb{P}_2$ 是由 $\mathbb{P}$ 通过分别添加 $x_1 + 1$ 与 x_1 所扩大的多项式组, 即

$$\mathbb{P}_1 = \mathbb{P} \cup \{x_1 + 1\}, \quad \mathbb{P}_2 = \mathbb{P} \cup \{x_1\}.$$

我们有下面的零点关系：

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{C}/I_1) \cup \mathrm{Zero}(\mathbb{P}_1) \cup \mathrm{Zero}(\mathbb{P}_2).$$

需要指出的是，在用 CharSet 计算特征列的过程中，必然会出现某些初式的多余因子. 这些因子应被删除，以便控制多项式的膨胀. 多余因子在计算多项式余式序列过程中的出现曾由柯林斯发现[19]. 李子明在 [50] 中研究了计算特征列过程中出现的多余因子.

定义 2.2.4 称升列 $\mathbb{C}$ 为非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 的 $\mathbb{Q}$ *修正特征列*, 如果

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) \subset \mathrm{Zero}(\mathbb{C}), \quad \mathrm{prem}(\mathbb{P}, \mathbb{C}) = \{0\},$$

其中 $\mathbb{Q}$ 为多项式组.

在 $\mathbb{Q} \subset \mathcal{K}$ 时，前缀 $\mathbb{Q}$ 将被略去.

现将算法 CharSet 作适当修改，使得在计算过程中可以抹去多项式的因子，并将所得算法记为 ModCharSet. 那么 ModCharSet 的输出是由升列 $\mathbb{C}$ 和一组抹去的互异因子 $\mathbb{F} = \{F_1, \cdots, F_t\}$ 构成. 显而易见， $\mathbb{C}$ 是输入多项式组 $\mathbb{P}$ 的 $\mathbb{F}$ 修正特征列. 因而，可对零点关系 (2.2.2) 作相应修改如下：

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{C}/\mathbb{I}) \cup \bigcup_{i=1}^{r} \mathrm{Zero}(\mathbb{P}_i) \cup \bigcup_{j=1}^{t} \mathrm{Zero}(\mathbb{Q}_j), \tag{2.2.4}$$

其中 $\mathbb{P}_i = \mathbb{P} \cup \{I_i\}$, $\mathbb{Q}_j = \mathbb{P} \cup \{F_j\}$. 又设 $H_1, \cdots, H_q$ 为任意选取的多项式，使得 $\mathrm{Zero}(\emptyset/H_1 \cdots H_q) = \mathrm{Zero}(\emptyset/\mathbb{I} \cup \mathbb{F})$, 那么 (2.2.4) 可由下式来替代：

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{C}/\mathbb{I}) \cup \bigcup_{k=1}^{q} \mathrm{Zero}(\mathbb{P} \cup \{H_k\}). \tag{2.2.5}$$

初式因子不可避免的出现经常使得所遇见的多项式太大而难于处理. 为抹去这些因子而频繁地尝试常常又耗费大量的计算时间.

注 2.2.1 弱基列与拟基列可以类似地定义. 计算多项式组 $\mathbb{P}$ 的弱基列或拟基列 $\mathbb{B}$ 的算法可以通过分别将算法 BasSet 中的最后一行用

$$\mathbb{F} \leftarrow \{F \in \mathbb{F} \setminus \{B\}\colon \ \mathrm{cls}(F) > \mathrm{cls}(B), \mathrm{ini}(F) \text{ 对 } B \text{ 是约化的}\}$$

或

$$\mathbb{F} \leftarrow \{F \in \mathbb{F} \setminus \{B\}\colon \ \mathrm{cls}(F) > \mathrm{cls}(B)\}$$

来替代而获得. 在基列被弱基列或拟基列代替后, 引理 2.2.3 和 CharSet 的说明仍然有效. 相应的 CharSet 所计算的弱升列或拟升列 $\mathbb{C}$ 分别称为 $\mathbb{P}$ 的 *弱特征列* 或 *拟特征列*.

良好三角列也被称为 *非矛盾 W 升列*. 任意单个非零常数多项式构成的集合都是 *矛盾 W 升列*. 周咸青和高小山在 [14, 16] 中称 W 升列为 *弱意义下的升链*, 并引进了 W-prem 的概念. 容易看出, 用相应的 W 升列和 W 基列来替换升列和基列, 我们可对算法 CharSet 作适当修改, 用以计算相应的 *W 特征列*.

我们将会看到, 特征列方法理论上在标准意义下比在其他弱意义下更加完整.

零点分解

现在让我们回到零点关系 (2.2.2). 由于每个 I_i 对 $\mathbb{C}$ 都是约化的, 根据引理 2.2.3, 多项式组 $\mathbb{P}_i \cup \mathbb{C}$ 的任意基列比 $\mathbb{C}$ 有较低的秩. 显然, $\mathrm{Zero}(\mathbb{P}_i \cup \mathbb{C}) = \mathrm{Zero}(\mathbb{P}_i)$. 因而, 视每一 $\mathbb{P}_i \cup \mathbb{C}$ 为 $\mathbb{P}$, 应用 CharSet 进一步计算其特征列, 并如此进行下去, 我们将在有限多步之后得到如下形式的零点分解:

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{C}_i/\mathbb{I}_i), \tag{2.2.6}$$

其中 $\mathbb{C}_i$ 都是升列, 且 $\mathbb{I}_i = \mathrm{ini}(\mathbb{C}_i)$.

定义 2.2.5 由 (弱) 升列 $\mathbb{C}_1, \cdots, \mathbb{C}_e$ 构成的有限集合或序列 Ψ 称为 $\mathcal{K}[\boldsymbol{x}]$ 中多项式组 $\mathbb{P}$ 的 *(弱) 特征序列*, 如果 (2.2.6) 式成立, 且对所有 i 有 $\mathrm{prem}(\mathbb{P}, \mathbb{C}_i) = \{0\}$.

$\Psi = \emptyset$ 意味着 $e = 0$, 因而 $\mathrm{Zero}(\mathbb{P}) = \emptyset$.

算法 CharSer: $\Psi \leftarrow \mathrm{CharSer}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算 $\mathbb{P}$ 的特征序列 Ψ.

C1. 命 $\Phi \leftarrow \{\mathbb{P}\}$, $\Psi \leftarrow \emptyset$.

C2. 重复下列步骤直至 $\Phi = \emptyset$:

C2.1. 从 Φ 中选取一个元素 $\mathbb{F}$, 且命 $\Phi \leftarrow \Phi \setminus \{\mathbb{F}\}$.

C2.2. 计算 $\mathbb{C} \leftarrow \mathrm{CharSet}(\mathbb{F})$.

C2.3. 若 $\mathbb{C}$ 不是矛盾列，则命

$$\Psi \leftarrow \Psi \cup \{\mathbb{C}\},$$
$$\Phi \leftarrow \Phi \cup \{\mathbb{F} \cup \mathbb{C} \cup \{I\}:\ I \in \mathrm{ini}(\mathbb{C}) \setminus \mathcal{K}\}.$$

事实上，该算法从 $\mathbb{P}$ 计算出一棵多枝树，称之为 $\mathbb{P}$ 的 *分解树*. 树的根部是 $\mathbb{P}$ 及其特征列 $\mathbb{C}$. 它在每一节点处通过添加初式而生成扩大了的多项式组及其特征列进行分叉. 该分解树如图 2 所示.

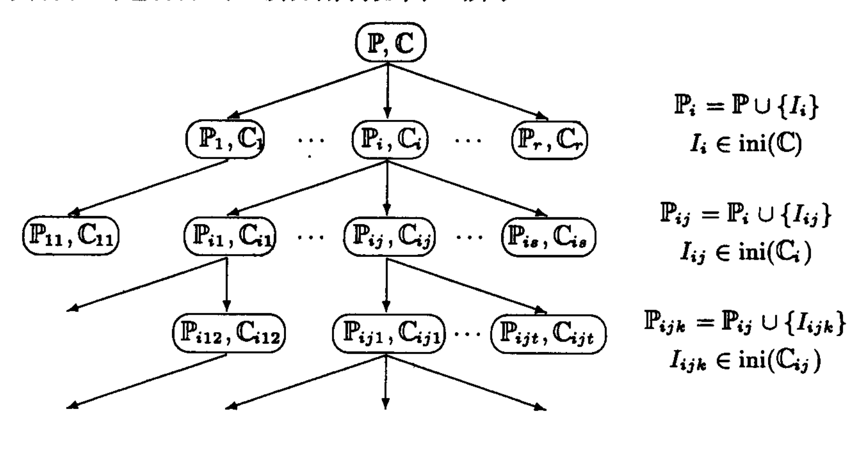


图 2 $\mathbb{P}$ 的分解树

例 2.2.4 如例 2.2.3 中一样，命 $\mathbb{P} = \{F_1, F_2, F_3\}$, 并设 $\mathbb{C}$ 为 $\mathbb{P}$ 的特征列. 容易求得 $\mathbb{P}_1 \cup \mathbb{C}$ 的特征列 $\mathbb{C}_1$ 和 $\mathbb{P}_2 \cup \mathbb{C}$ 的特征列 $\mathbb{C}_2$ 如下：

$$\mathbb{C}_1 = [x_1 + 1, x_2, x_3^2 - 1, x_4 - x_3],$$
$$\mathbb{C}_2 = [x_1, 2\,x_2^2 + 1, x_3, x_4^2 - x_2x_4 + 3\,x_2].$$

注意，$\mathbb{C}_1$ 和 $\mathbb{C}_2$ 中所有多项式的初式都为常数. 因此我们得到了 $\mathbb{P}$ 的特征序列 $\Psi = \{\mathbb{C}, \mathbb{C}_1, \mathbb{C}_2\}$ 以及如下形式的零点分解：

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{C}/I_1) \cup \mathrm{Zero}(\mathbb{C}_1) \cup \mathrm{Zero}(\mathbb{C}_2).$$

注 2.2.2 设 $\mathbb{C}$ 为 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 的特征列，而 P 为 $\mathcal{K}[\boldsymbol{x}]$ 中任一对 $\mathbb{C}$ 约化的多项式. $\mathbb{P} \cup \{P\}$ 的基列和特征列都不一定比 $\mathbb{C}$ 有较低的秩. 举例来说，令

$$\mathbb{P} = \{x_1^2, x_1^2 + x_1, x_1x_2, x_2x_3\}.$$

对于序 $x_1 \prec x_2 \prec x_3$,

$$\mathbb{B} = [x_1^2, x_1x_2], \quad \mathbb{C} = [x_1, x_2x_3]$$

分别是 $\mathbb{P}$ 的基列和特征列. 此时 x_2 对 $\mathbb{C}$ 是约化的, 可是 $\mathbb{P}\cup\{x_2\}$ 的基列与 $\mathbb{B}$ 具有相同的秩.

作为另一个例子, 考虑多项式组

$$\mathbb{P}=\{x_1^2-x_2^2,x_1^2-2\,x_2^2,x_2^2\}.$$

$\mathbb{P}$ 的一特征列为 $\mathbb{C}=[x_1^2,x_2^2]$. 很明显, x_1x_2 对 $\mathbb{C}$ 是约化的. 现在, $[x_1^3,x_1x_2]$ 是 $\mathbb{P}\cup\{x_1x_2\}$ 的特征列, 且比 $\mathbb{C}$ 有较高的秩.

以上两例说明为何在 CharSer 的最后一行 $\mathbb{C}$ 不能从 $\mathbb{F}\cup\mathbb{C}\cup\{I\}$ 中略去. 但是, 如果假设 *在 $\mathbb{P}^*$ 的基列与 $\mathbb{P}$ 的基列 $\mathbb{B}$ 同秩时, $\mathbb{B}$ 总是选作 $\mathbb{P}^*\supset\mathbb{P}$ 的基列*, 那么在用 $\mathbb{F}\cup\{I\}$ 代替 $\mathbb{F}\cup\mathbb{C}\cup\{I\}$ 后, 这节和以后章节中所讨论的各种特征序列算法仍能保证终止.

注 2.2.3 算法 CharSer 在弱和拟意义下仍然适用. 换句话说, 多项式组的弱或拟特征序列可以用这一算法通过将特征列分别换成弱或拟特征列而求得. 但是, 在拟意义下该算法不一定终止.

在计算特征序列的过程中, 扩大多项式组的循环生成可使分解树产生大量分支. 其中有些分支完全是多余的, 应该被切除. 人们引进了各种技巧用以控制分支的扩张 (参阅 [16, 83]). 例如: 在图 2 中, 如果根节点在某一 $\mathbb{P}_i$ 的树枝已经被计算出来, 那么对包含 $\mathbb{P}_i$ 的任意多项式组 $\mathbb{P}_j$ 由 $\mathbb{P}_j$ 生出的树枝都无需进一步考虑.

推广与扩充

在算法 CharSet 中, 每个扩大了的多项式组 $\mathbb{F}_{i+1}$ —— 如图 (2.2.3) 所示 —— 都是 $\mathbb{F}_i$ 与 $\mathbb{R}_i$ 的并. 随着 i 的递增, $\mathbb{F}_{i+1}$ 中多项式的个数迅续增加. 为减少计算量, 策略之一是命 $\mathbb{F}_{i+1}$ 仅为 $\mathbb{B}_i$ 与 $\mathbb{R}_i$ 的并, 最后再检查是否 $\mathbb{P}$ 中的所有多项式对最后一个基列的伪余式都为 0. 这一策略由吴在 [100, 101] 中提出. 我们在本小节的前一半中将该策略描述为广义特征列算法, 它可以导致标准算法的若干变形.

定义 2.2.6 设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的非空多项式组. 任意包含于 Ideal($\mathbb{P}$) 的升列 —— 其秩不高于 $\mathbb{P}$ 的基列的秩 —— 都称为 $\mathbb{P}$ 的 *中间列*.

称 $\mathbb{P}$ 的中间列 $\mathbb{M}$ 为 $\mathbb{P}$ 的 *特征列*, 如果 $\mathrm{prem}(\mathbb{P},\mathbb{M})=\{0\}$.

显而易见, $\mathbb{P}$ 的任意基列都是它的中间列. 这里所说的特征列与定义 2.2.3 中给出的特征列是一致的.

引理 2.2.4 设非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 有

$$\mathbb{M} = [M_1, M_2, \cdots, M_r]$$

为其中间列，这里 $\mathrm{cls}(M_1) > 0$. 如果 M 是一对 $\mathbb{M}$ 约化的非零多项式，那么多项式组 $\mathbb{P}^+ = \mathbb{P} \cup \mathbb{M} \cup \{M\}$ 的任意中间列 $\mathbb{M}^+$ 都比 $\mathbb{M}$ 有较低的秩.

证 设 $\mathbb{B}^+$ 与 $\mathbb{B}^*$ 分别为 $\mathbb{P}^+$ 与 $\mathbb{P} \cup \mathbb{M}$ 的基列，那么 $\mathbb{B}^* \precsim \mathbb{M}$. 若 $\mathbb{B}^* \sim \mathbb{M}$, 则 M 对 $\mathbb{B}^*$ 是约化的. 所以，由定义 2.2.6 和引理 2.2.3 知

$$\mathbb{M}^+ \precsim \mathbb{B}^+ \prec \mathbb{B}^* \sim \mathbb{M}.$$

若 $\mathbb{B}^* \prec \mathbb{M}$, 则

$$\mathbb{M}^+ \precsim \mathbb{B}^+ \precsim \mathbb{B}^* \prec \mathbb{M}$$

成立. 因此在任一情形都有 $\mathbb{M}^+ \prec \mathbb{M}$. □

我们以 GenCharSet 表示由 CharSet 通过将其 C2.1 用下列步骤来替换所得的算法：

C2.1. 计算 $\mathbb{F}$ 的中间列 $\mathbb{C}$.

定理 2.2.5 算法 GenCharSet 终止，其说明是正确的. 换言之，该算法计算任给非空多项式组 $\mathbb{P}$ 的特征列 $\mathbb{C}$.

证 算法 GenCharSet 与 CharSet 具有相同的结构. 如果将每个 $\mathbb{B}_i$ 都用 $\mathbb{F}_i$ 的任意中间列 $\mathbb{M}_i$ 来替换，且命每个扩大了的多项式组 $\mathbb{F}_{i+1}$ 为 $\mathbb{F}_i \cup \mathbb{R}_i \cup \mathbb{M}_i$, 我们应得到一个与 (2.2.3) 类似的图解，但 $\mathbb{M}_i$ 不一定是 $\mathbb{F}_i$ 的子集. 因此 GenCharSet 的终止性由引理 2.2.1 和 2.2.4 所保证. 由 $\mathbb{F}_i$ 及伪余公式的构造可知，算法的正确性容易用类似于 CharSet 的正确性论证来加以证明. □

通过使用不同的中间列，我们可以得到算法 CharSet 的不同变形. 如果用基列作中间列，那么 GenCharSet 与 CharSet 恒同. 现以 CharSetN 表示由 CharSet 通过将其最后一行中的 $\mathbb{F} \cup \mathbb{R}$ 用 $\mathbb{C} \cup \mathbb{R}$ 来替换所得的算法，那么 CharSetN 计算输入多项式组的中间列. 又将 GenCharSet 中的步骤 C2.1 用

C2.1. 计算 $\mathbb{C} \leftarrow \mathrm{CharSetN}(\mathbb{F})$.

来替换，我们立即得到本小节开始时所提到的对 CharSet 的修改.

如果我们只想计算三角列，特征列算法则有更多变形的余地. 各种对 CharSet 的修改自然导致对特征序列算法的修改，对此我们略去有关细节. 对特征列算法的变形、修改及扩充，读者也可参阅 [14, 42, 16] 及其相关工作.

设 $[\mathbb{P},\mathbb{Q}]$ 为一多项式系统. 由 (2.2.6) 可得如下零点分解:

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{C}_i/\mathbb{I}_i \cup \mathbb{Q}), \tag{2.2.7}$$

其中每个 $\mathbb{C}_i$ 都为升列，且 $\mathbb{I}_i = \mathrm{ini}(\mathbb{C}_i)$. 在 (2.2.7) 式中，若对某一 i 有 $0 \in \mathrm{prem}(\mathbb{Q},\mathbb{C}_i)$，则可将分支 $\mathrm{Zero}(\mathbb{C}_i/\mathbb{I}_i \cup \mathbb{Q})$ 删除. 于是我们可以假定 $0 \notin \mathrm{prem}(\mathbb{Q},\mathbb{C}_i)$ 对所有 i 成立. 而且，我们可以用 $\mathbb{D}_i = \mathbb{I}_i \cup \mathrm{prem}(\mathbb{Q},\mathbb{C}_i)$ 来替换 (2.2.7) 中的 $\mathbb{I}_i \cup \mathbb{Q}$，使得

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{C}_i/\mathbb{D}_i), \tag{2.2.8}$$

这里 $[\mathbb{C}_i,\mathbb{D}_i]$ 明显是良好三角系统.

定义 2.2.7　$\mathcal{K}[\boldsymbol{x}]$ 中的任意 (良好) 三角系统 $\mathfrak{T}_1,\cdots,\mathfrak{T}_e$ 构成的有限集合或序列 Ψ 都称为 *(良好) 三角序列*. 如果 (2.1.7) 式对 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $\mathfrak{P}$ 成立，则称该序列为 $\mathfrak{P}$ 的 *(良好) 三角序列*.

$[\mathbb{P},\emptyset]$ 的 (良好) 三角序列也称为多项式组 $\mathbb{P}$ 的 *(良好) 三角序列*.

如果 (2.1.7) 式对 $\mathfrak{T}_i = [\mathbb{T}_i,\mathbb{U}_i]$ 成立，且对所有 i 有 $\mathrm{prem}(\mathbb{P},\mathbb{T}_i) = \{0\}$，则称 Ψ 为 $\mathfrak{P} = [\mathbb{P},\mathbb{Q}]$ 的 *特征序列*.

$\Psi = \emptyset$ 的情形理解为 $\mathrm{Zero}(\mathfrak{P}) = \emptyset$.

很明显，(2.2.8) 式中的良好三角系统 $[\mathbb{C}_1,\mathbb{D}_1],\cdots,[\mathbb{C}_e,\mathbb{D}_e]$ 组成的集合是 $[\mathbb{P},\mathbb{Q}]$ 的特征序列.

注 2.2.4　*弱中间列* 和 *拟中间列* 可以类似地定义. 在 GenCharSet 中将中间列换成弱中间列或拟中间列，所得的算法可以用来计算相应的弱或拟特征列. 也可设计出类似的算法用以计算多项式组或系统的弱特征序列.

注 2.2.5　用 CharSetN 从 $\mathbb{P}$ 算出的 (弱、拟) 中间列称为 $\mathbb{P}$ 的 *(弱、拟) 近特征列*. 对任意 (弱、拟) 近特征列 $\mathbb{C}$，零点关系式 (2.2.4) 和 (2.2.5) 不再成立；我们仅有

$$\mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(\mathbb{C}).$$

值得注意的是，对有些应用如解代数方程，计算 (弱、拟) 近特征列就足够了. 特别是如果 $\mathbb{C}$ 只有有限多个零点，是否 $\mathbb{C}$ 的每个零点也是 $\mathbb{P}$ 的零点可以通过代入求值予以验证.

注 2.2.6 为了确定 (弱、拟) 近特征列 $\mathbb{C}$ 是否为 (弱、拟) 特征列，我们需要遵循算法 GenCharSet 的步骤来验证是否输入组中的所有多项式对 $\mathbb{C}$ 的伪余式都为 0. 实验表明，在大多数情形这些伪余式确实为 0, 即 GenCharSet 在第一个循环之后便终止. 但是 0 伪余式的验证经常占用大量的计算时间. 有一些策略可用来部分地避免 0 伪余式的验证. 其一是通过检验某些初式与被抹去的因子之间的因子关系来实现的 (见 [79]).

本书中所给出的大部分算法都已由作者在流行的计算机代数系统 Maple 中实现. 特别是 CharSets 软件包，它实施了一系列基于特征列的算法，并被收入 Maple 的共享程序库，自 1991 年早春以来对外公开发行. 该软件包的最新版本可以从万维网上获取：

`http://calfor.lip6.fr/~wang/charsets.html`

本书侧重于理论和算法的发展. 我们将不讨论实施细节，也不提供实验统计结果以及算法之间的比较. 至于这方面的信息，读者可以查阅有关研究论著. 然而，本书中给出了诸多注记，作为对算法有效实施的提示. 一般来说，只关心理论方面的读者可以跳过这些注记.

2.3 改良的赛登贝格算法

本节的目的在于介绍一种零点分解算法，它在每次作伪除时都将多项式系统分裂. 使用这一算法，所计算的是三角序列，而不是特征序列. 这样做的优点之一是完全避免了对 0 伪余式的检验. 我们采用纯粹由上至下 (即从 x_n 到 x_1) 的步骤消元，这一策略实质上属于塞登贝格 [63, 64]. 与之相比，算法 CharSet 中的消元可被认为是对所有变元同时进行的.

由于非良好的三角列可以有不良行为，在拟意义下对特征列建立完整的理论是不可能的. 在标准或弱意义下，特征列的计算常常导致多项式迅速增大. 其主要原因是，在这种情形每个多项式或其初式需要对升列中的其他多项式是约化的. 为了控制多项式的大小以及其他原因，我们使用三角系统 $[\mathbb{T}, \mathbb{U}]$, 其中 $\mathbb{U}$ 收集所有 $\mathrm{prem}(I, \mathbb{T})$, $\forall I \in \mathrm{ini}(\mathbb{T})$, 及其他多项式.

此外，像 CharSer 中那样计算 $\mathbb{P} \cup \{I\}$ 的特征列，一些在计算 $\mathbb{P}$ 的特征列 $\mathbb{C}$ 时已经作过的伪除可能会被重作. 换句话说，在算法 CharSer 的运行过

程中会有伪余式的重复计算，而这是不必要的. 为了避免这些重复以及为随后的计算留下尽可能多的信息量，我们将通过数据结构三元组和四元组来保留已部分三角化的系统.

在描述消去算法之前，我们先来证明下面的简单引理.

引理 2.3.1 设 T 为 $\mathcal{K}[\boldsymbol{x}]$ 中的非常数多项式，$[\mathbb{P},\mathbb{Q}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统，而 $\mathrm{ini}(T)=I$, $\mathbb{R}=\mathrm{prem}(\mathbb{P},T)\setminus\{0\}$, 那么

$$\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q})=\mathrm{Zero}(\mathbb{R}\cup\{T\}/\mathbb{Q}\cup\{I\})\cup\mathrm{Zero}(\mathbb{P}\cup\{I,\mathrm{red}(T)\}/\mathbb{Q}). \quad (2.3.1)$$

证 对任意多项式 $P\in\mathbb{P}$, 用 T 对 P 关于 x_i 作伪除给出伪余公式如下:

$$I^qP=AT+R, \quad (2.3.2)$$

这里 $A,R\in\mathcal{K}[\boldsymbol{x}]$ 且整数 $q>0$. 对任意 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q})$, 我们有

$$T(\bar{\boldsymbol{x}})=0,\quad P(\bar{\boldsymbol{x}})=0,\quad \forall P\in\mathbb{P},$$

因而对所有 $R\in\mathbb{R}$ 有 $R(\bar{\boldsymbol{x}})=0$. 明显地，$Q(\bar{\boldsymbol{x}})\neq 0$ 对所有 $Q\in\mathbb{Q}$ 成立. 若 $I(\bar{\boldsymbol{x}})\neq 0$, 则

$$\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{R}\cup\{T\}/\mathbb{Q}\cup\{I\}). \quad (2.3.3)$$

否则，我们有 $I(\bar{\boldsymbol{x}})=0$; 因此 $\mathrm{red}(T)(\bar{\boldsymbol{x}})=0$. 所以

$$\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}\cup\{I,\mathrm{red}(T)\}/\mathbb{Q}). \quad (2.3.4)$$

这说明 (2.3.1) 式的左边包含于右边. 为了证明相反方向，我们注意，如果 $\bar{\boldsymbol{x}}$ 满足 (2.3.4) 式，则 $T(\bar{\boldsymbol{x}})=0$; 因而 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q})$. 否则，假设 (2.3.3) 式成立. 依 (2.3.2), 对所有 $P\in\mathbb{P}$ 有 $P(\bar{\boldsymbol{x}})=0$. 于是 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q})$ 也成立. □

对任意整数 $1\leq i\leq n$ 及多项式组 $\mathbb{P}$, $\mathbb{P}$ 中只含有变元 $x_1,\cdots,x_i$ 的多项式构成的集合记作 $\mathbb{P}^{(i)}$. 用符号来表达，我们有

$$\mathbb{P}^{(i)}\triangleq\mathbb{P}\cap\mathcal{K}[x_1,\cdots,x_i].$$

又命

$$\mathbb{P}^{[i]}\triangleq\mathbb{P}\setminus\mathbb{P}^{(i)},\quad \mathbb{P}^{\langle i\rangle}\triangleq\mathbb{P}^{(i)}\setminus\mathbb{P}^{(i-1)}.$$

对任意多项式系统 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$, 定义

$$\mathfrak{P}^{(i)} \triangleq [\mathbb{P}^{(i)},\mathbb{Q}^{(i)}],\quad \mathfrak{P}^{\langle i\rangle} \triangleq [\mathbb{P}^{\langle i\rangle},\mathbb{Q}^{\langle i\rangle}].$$

我们称多项式组 $\mathbb{P}$ 的 *级* 为 i, 记作 $\mathrm{level}(\mathbb{P})=i$, 如果 $\mathbb{P}\subset\mathcal{K}[x_1,\cdots,x_i]$ 且 $\mathbb{P}^{\langle i\rangle}\neq\emptyset$, 即 i 是使得 $\mathbb{P}\subset\mathcal{K}[x_1,\cdots,x_i]$ 的最小整数. $\mathbb{P}$ 的级也称为 $\mathfrak{P}$ 的级.

现在我们引进一个称之为 *三元组* 的数据结构, 它将在若干算法的描述中使用.

数据结构 一个级为 i $(1\le i\le n)$ 的 *三元组* 是一含有三个元素的表格 $[\mathbb{P},\mathbb{Q},\mathbb{T}]$, 其中

(a) $[\mathbb{P},\mathbb{Q}]$ 是 $\mathcal{K}[\boldsymbol{x}]$ 中级为 i 的多项式系统;

(b) $\mathbb{T}$, 若非空, 则是 $\mathcal{K}[\boldsymbol{x}]$ 中的三角列, 且使 $\mathbb{T}^{(i)}=\emptyset$.

在说到多项式系统 $[\mathbb{P},\mathbb{Q}]$ 时, 我们关心的是零点集 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. 显然对每个 i, $\mathbb{P}$ 都可以写成 $\mathbb{P}=\mathbb{P}^{(i)}\cup\mathbb{P}^{[i]}$. 可能发生的是, 对某一 i, $\mathbb{P}^{(i)}$ 的级为 i 且 $\mathbb{P}^{[i]}$ 能经过排序变成三角列 $\mathbb{T}$. 这时 $[\mathbb{P}^{(i)},\mathbb{Q},\mathbb{T}]$ 够成一个三元组, 而 $\mathrm{Zero}(\mathbb{P}^{(i)}\cup\mathbb{T}/\mathbb{Q})$ 正是我们的兴趣所在.

我们的消去程序将从一个三元组 $[\mathbb{P},\mathbb{Q},\mathbb{T}]$ 开始, 其中 $\mathbb{T}=\emptyset$. 对 $i=n,n-1,\cdots,1$, 变元 x_i 被逐个消去, 所得的、三角化的多项式被添入 $\mathbb{T}$.

设 i 为一正整数, $[\mathbb{P},\mathbb{Q}]$ 是级为 i 的多项式系统. 明显地, $\mathbb{F}=\mathbb{P}^{\langle i\rangle}\neq\emptyset$, 且 $\mathbb{F}$ 中所有多项式的类都为 i. 我们想将变元 x_i 从 $\mathbb{F}$ 的多项式中消去, 使得消元之后只有一个多项式的类为 i. 为此, 我们从 $\mathbb{F}$ 中选取一个关于 x_i 次数最低的多项式 T, 并用 T 对 $\mathbb{F}\setminus\{T\}$ 中所有多项式关于 x_i 作伪除. 同时, 假定 $\mathrm{ini}(T)$ 不为零; $\mathrm{ini}(T)$ 为零的情形则通过用 $\mathrm{ini}(T)$ 和 $\mathrm{red}(T)$ 来替换 T 而另行处理. 然后, 我们将 $\mathbb{F}$ 重新赋值为 $\{T\}\cup\mathrm{prem}(\mathbb{F},T)\setminus\{0\}$, 再重复上述过程. 这样下去, 我们最终将得到 ($\mathbb{F}$ 中) 单个类为 i 的多项式 T, 以及一组级 $\le i$ 的其他多项式系统.

上面所解释的程序可按算法的形式描述如下.

算法 Elim: $[T,\mathbb{F},\mathbb{G},\Delta]\leftarrow\mathrm{Elim}(\mathbb{P},\mathbb{Q},i)$. 给定整数 $i>0$ 和 $\mathcal{K}[\boldsymbol{x}]$ 中级为 i 的多项式系统 $[\mathbb{P},\mathbb{Q}]$, 本算法计算类为 i 的多项式 T, 级 $\le i-1$ 的多项式系统 $[\mathbb{F},\mathbb{G}]$ 和一组级 $\le i$ 的多项式系统 Δ, 使得

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q})=\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G})\cup\bigcup_{[\mathbb{P}^*,\mathbb{Q}^*]\in\Delta}\mathrm{Zero}(\mathbb{P}^*/\mathbb{Q}^*).\qquad(2.3.5)$$

E1. 命 $T \leftarrow 0, \mathbb{F} \leftarrow \mathbb{P}, \mathbb{G} \leftarrow \mathbb{Q}, \Delta \leftarrow \emptyset$.

E2. 重复下列步骤直至 $\mathbb{F}^{\langle i\rangle} = \{T\}$:

E2.1. 从 $\mathbb{F}^{\langle i\rangle}$ 中选取一个关于 x_i 次数最低的多项式 T.

E2.2. 命

$$\Delta \leftarrow \Delta \cup \{[\mathbb{F} \setminus \{T\} \cup \{\mathrm{red}(T), \mathrm{ini}(T)\}, \mathbb{G}]\},$$
$$\mathbb{G} \leftarrow \mathbb{G} \cup \{\mathrm{ini}(T)\}.$$

E2.3. 计算 $\mathbb{F} \leftarrow \{T\} \cup \mathrm{prem}(\mathbb{F}, T) \setminus \{0\}$.

E3. 命 $\mathbb{F} \leftarrow \mathbb{F} \setminus \{T\}$.

证 由于 $\mathbb{P}$ 的级为 i, $\mathbb{F}^{\langle i\rangle}$ 在开始时既非空也不等于 $\{T\} = \{0\}$. 容易看出, E2 的每一子步骤都终止. 对 E2 的每个循环, $\deg(T, x_i)$ 至少减 1. 所以在有限步之后, $\mathbb{F}$ 中多项式对 T 的所有非零伪余式的类都将 $< i$. 此时集合 $\mathbb{F}^{\langle i\rangle}$ 变为 $\{T\}$ 而使 E2 的循环终止.

重复使用引理 2.3.1 中的 (2.3.1) 式即得零点关系 (2.3.5). □

在 $\mathrm{ini}(T)$ 为常数时, 步骤 E2.2 可以跳过; 而在步骤 E2.3 中, 实际上只有 $\mathbb{F}^{[i-1]} \setminus \{T\}$ 中多项式的伪余式需要计算.

例 2.3.1 在文献 [81] 中作为例子我们曾讨论过多项式组

$$\mathbb{P} = \{x^{31} - x^6 - x - y, x^8 - z, x^{10} - t\}.$$

据特拉弗索和多纳蒂的论文称, 是罗比阿诺使该多项式组广为流传. 它将在这里以及其他地方用来说明若干算法. 不难发现, 关于变元序 $x \prec y \prec z \prec t$, $\mathbb{P}$ 已是三角列. 但为了说明的需要, 我们将变元排序为 $t \prec z \prec y \prec x$.

为了演示 Elim 如何工作, 我们将级为 4 的多项式系统 $[\mathbb{P}, \emptyset]$ 作为输入. 最初, 在步骤 E1 中命

$$T \leftarrow 0, \quad \mathbb{F} \leftarrow \mathbb{P}, \quad \mathbb{G} \leftarrow \emptyset, \quad \Delta \leftarrow \emptyset.$$

现在进入循环 E2. 首先, 如步骤 E2.1 所示, 从 $\mathbb{F}^{[3]} = \mathbb{F}$ 中选取关于 x 次数最低的多项式 $T = x^8 - z$; 其次数是 8, 且初式为 $I = 1$. 由于 I 是常数, 我们可以跳过步骤 E2.2. 用 T 伪除 $\mathbb{F} = \mathbb{P}$ 中的另外两个多项式, 我们得到两个非零伪余式

$$R_1 = z^3x^7 - x^6 - x - y, \quad R_2 = zx^2 - t,$$

这里 $\mathrm{lv}(R_1) = \mathrm{lv}(R_2) = x$. 所以在 E2.3 中，更新 $\mathbb{F} \leftarrow \{T, R_1, R_2\}$.

在第二个循环步骤 E2.1 中，从 $\mathbb{F}^{[3]} = \mathbb{F}$ 中选取关于 x 次数最低的多项式 $T = R_2$; 其次数为 2, 初式为 $I = z$. 在 E2.2 中，命

$$\Delta \leftarrow \{[\{x^8 - z, R_1, z, -t\}, \emptyset]\}, \quad \mathbb{Q} \leftarrow \{z\}.$$

类似地，用 $T = R_2$ 伪除 $\mathbb{F}$ 中的另外两个多项式得伪余式

$$R_3 = -z^5 + t^4, \quad R_4 = t^3z^3x - z^3x - z^3y - t^3,$$

这里 $\mathrm{lv}(R_3) = z$, $\mathrm{lv}(R_4) = x$. 然后，在 E2.3 中置 $\mathbb{F} \leftarrow \{R_2, R_3, R_4\}$.

关于第三个循环，在 E2.1 中置 $T \leftarrow R_4$, 此时 $\deg(R_4, x) = 1 < \deg(R_2, x)$, 并可用 $z \in \mathbb{Q}$ 将 R_4 的初式 $t^3z^3 - z^3$ 化简为 $I = t^3 - 1$. 在 E2.2 中，将多项式系统

$$[\{R_2, R_3, -z^3y - t^3, t^3 - 1\}, \{z\}]$$

添入 Δ, 多项式 $t^3 - 1$ 添入 $\mathbb{Q}$. 用 $T = R_4$ 伪除 R_2, 我们有

$$R_5 = \mathrm{prem}(R_2, R_4) = z^6y^2 + 2\,t^3z^3y - t^7z^5 + 2\,t^4z^5 - tz^5 + t^6$$

及 $\mathrm{lv}(R_5) = y$. 最后，命 $\mathbb{F} \leftarrow \{R_4, R_3, R_5\}$, 并终止循环步骤 E2.

在 E3 中将 T 从 $\mathbb{F}$ 中删除之后，整个算法终止. 输出为 $T = R_4$, 多项式系统

$$[\mathbb{F}, \mathbb{G}] = [\{R_3, R_5\}, \{z, t^3 - 1\}],$$

以及另外两个多项式系统组成的集合 Δ.

现在，让我们来说明如何以 Elim 为主要子算法将多项式系统 $[\mathbb{P}, \mathbb{Q}]$ 分解为三角系统. 这是通过由上至下即从 x_n 到 x_1 的消元来实现的. 具体来说，对每个 x_i, $i = n, \cdots, 1$, 我们按如下方式进行.

如果 $\mathbb{P}^{\langle i \rangle} = \emptyset$, 则转向下一个 i. 否则，设 $T \in \mathbb{P}^{\langle i \rangle}$ 关于 x_i 的次数最低. 那么

$$\mathbb{P} = 0, \mathbb{Q} \neq 0 \iff \begin{cases} \mathbb{P}^* = 0, I = 0, \mathrm{red}(T) = 0, & \mathbb{Q} \neq 0; \text{ 或} \\ \mathrm{prem}(\mathbb{P}, T) = 0, T = 0, & \mathbb{Q} \neq 0, I \neq 0, \end{cases}$$

这里

$$\mathbb{P}^* = \mathbb{P} \setminus \{T\}, \quad I = \mathrm{ini}(T).$$

因此，我们有

$$\begin{aligned}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) &= \mathrm{Zero}(\mathbb{P}^* \cup \{I, \mathrm{red}(T)\}/\mathbb{Q}) \\ &\quad \cup \mathrm{Zero}(\mathrm{prem}(\mathbb{P}, T) \cup \{T\}/\mathbb{Q} \cup \{I\}) \\ &= \cdots \qquad\qquad (\text{递归重复}) \\ &= \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i).\end{aligned}$$

下面的算法将以上概述精确化.

算法 TriSer: $\Psi \leftarrow \mathrm{TriSer}(\mathbb{P}, \mathbb{Q})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P}, \mathbb{Q}]$，本算法计算 $[\mathbb{P}, \mathbb{Q}]$ 的良好三角序列 Ψ.

T1. 命 $\Psi \leftarrow \emptyset$, $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, \emptyset]\}$.

T2. 重复下列步骤直至 $\Phi = \emptyset$:

T2.1. 从 Φ 中选取三元组 $[\mathbb{F}, \mathbb{G}, \mathbb{T}']$, 且命 $\Phi \leftarrow \Phi \setminus \{[\mathbb{F}, \mathbb{G}, \mathbb{T}']\}$.

T2.2. 计算 $[\mathbb{T}, \mathbb{U}, \Omega] \leftarrow \mathrm{PriTriSys}(\mathbb{F}, \mathbb{G})$.

T2.3. 命

$$\Phi \leftarrow \Phi \cup \{[\mathbb{F}^*, \mathbb{G}^*, \mathbb{T}^* \cup \mathbb{T}']: [\mathbb{F}^*, \mathbb{G}^*, \mathbb{T}^*] \in \Omega\}.$$

若 $\mathbb{T} \neq [1]$, 则命 $\Psi \leftarrow \Psi \cup \{[\mathbb{T} \cup \mathbb{T}', \mathbb{U}]\}$.

其中子算法 PriTriSys 叙述如下.

算法 PriTriSys: $[\mathbb{T}, \mathbb{U}, \Omega] \leftarrow \mathrm{PriTriSys}(\mathbb{P}, \mathbb{Q})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P}, \mathbb{Q}]$, 本算法计算 (良好三角系统) $[\mathbb{T}, \mathbb{U}]$ 和三元组集合 Ω, 使得

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \mathrm{Zero}(\mathbb{T}/\mathbb{U}) \cup \bigcup_{[\mathbb{P}^*, \mathbb{Q}^*, \mathbb{T}^*] \in \Omega} \mathrm{Zero}(\mathbb{P}^* \cup \mathbb{T}^*/\mathbb{Q}^*).$$

P1. 命 $\mathbb{T} \leftarrow \emptyset$, $\mathbb{F} \leftarrow \mathbb{P}$, $\mathbb{U} \leftarrow \mathbb{Q}$, $\Omega \leftarrow \emptyset$.

P2. 对 $i = \mathrm{level}(\mathbb{P}), \cdots, 1$ 执行下列步骤:

P2.1. 如果 $\mathbb{F} \cap \mathcal{K} \setminus \{0\} \neq \emptyset$, 则命 $\mathbb{T} \leftarrow [1]$, 且算法终止. 若 $\mathrm{level}(\mathbb{F}) < i$, 则返回 P2 执行下一个 i.

P2.2. 计算 $[T, \mathbb{F}, \mathbb{U}, \Delta] \leftarrow \mathrm{Elim}(\mathbb{F}, \mathbb{U}, i)$, 且命

$$\Omega \leftarrow \Omega \cup \{\delta \cup [\mathbb{T}]:\ \delta \in \Delta\}.$$

P2.3. 计算 $\mathbb{U} \leftarrow \mathrm{prem}(\mathbb{U}, T)$.

P2.4. 若 $0 \in \mathbb{U}$, 则命 $\mathbb{T} \leftarrow [1]$, 且算法终止; 否则命 $\mathbb{T} \leftarrow [T] \cup \mathbb{T}$.

在 TriSer 的 T2 中, 集合 Φ 中的三元组既递增又递减, 同时生成三角系统 $[\mathbb{T}, \mathbb{U}]$. 这一程序在 Φ 变成空集时终止. 在循环步骤 T2 之内, 对从 Φ 中选取的级为 ℓ 的每个三元组 $[\mathbb{F}, \mathbb{G}, \mathbb{T}]$, 子算法 Elim 将变元从 x_ℓ 到 x_1 依次消去.

和前面一样, 如果 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$ 在 TriSer 中得到确认, 则有 $e = 0$ 以及 $\Psi = \emptyset$.

例 2.3.2 让我们回到例 2.3.1, 并用输入系统 $[\mathbb{P}, \emptyset]$ 来演示 TriSer. 集合 Ψ 和 Φ 的初始值分别设为 $\emptyset$ 和 $\{[\mathbb{P}, \emptyset, \emptyset]\}$.

考虑循环步骤 T2. 首先, 在 T2.1 中选取 Φ 中仅有的三元组, 并将其从 Φ 删除. 我们进入步骤 T2.2 中的 PriTriSys; 先考虑迭代 $i = 4$. 在 P2.2 中调用 Elim 产生例 2.3.1 中给出的多项式 $T = R_4$, 多项式系统

$$[\mathbb{F}, \mathbb{G}] = [\{R_3, R_5\}, \{z, t^3 - 1\}],$$

以及集合 Δ. 因此, 可由 Δ 中的两个多项式系统生成两个三元组, 并将其添入 Φ.

由于 $\mathbb{G}$ 中两个多项式的导元都 $\prec x$, 步骤 P2.3 的执行是平凡的 —— 它不改变任何变量的值. 在 P2.4 中, 命 $\mathbb{T} \leftarrow [R_4]$.

对 $i = 3$ 和 2, $\mathbb{F}$ 中的多项式 R_5 和 R_3 分别在 P2.2 中选作 T; 此时无需消元. 由于 $\mathbb{G}$ 中两个多项式对 R_5 和 R_3 的伪余式均为其自身, $\mathbb{G}$ 在 P2.3 中不会更改. 因而我们得到第一个三角系统 $[\mathbb{T}_1, \mathbb{U}_1]$, 其中

$$\mathbb{T}_1 = [R_3, R_5, R_4], \quad \mathbb{U}_1 = \{z, t^3 - 1\}.$$

该三角系统在 T2.3 中被添入 Ψ.

现在 Φ 中剩下两个需要考虑的三元组. 对其中的 $[\{T, R_1, z, -t\}, \emptyset, \emptyset]$, 多项式 T 与 R_1 都具有导元 x, 其中 R_1 有较低的次数 7, 它的初式为 $z^3 \rightsquigarrow z$. 这里和其他地方, $\rightsquigarrow$ 的意思是 "被化简为". 我们可以严格遵循所描述的算法, 根据 $z = 0$ 和 $z \neq 0$ 将计算分为两种情形. 这样做稍微有点复杂. 事实上, 我

们可以用 $z=0$ 和 $t=0$ 对 T 与 R_1 进行化简，并将所得的多项式变成无平方因子．由此立即可得第二个三角列 $\mathbb{T}_2=[t,z,y,x]$，而 $\mathbb{U}_2=\emptyset$．至于剩下的三元组

$$[\mathbb{F},\mathbb{G},\mathbb{T}]=[\{R_3,R_2,-z^3y-t^3,t^3-1\},\{z\},\emptyset],$$

多项式

$$R_2,\quad -z^3y-t^3,\quad R_3,\quad t^3-1$$

的导元分别为 x,y,z,t，因而它们已构成三角列．于是我们得到

$$\mathbb{T}_3=[t^3-1,R_3,-z^3y-t^3,R_2],\quad \mathbb{U}_3=\{z\}.$$

TriSer 的证明　*终止性*．我们只需证明循环 T2 终止．考虑在 TriSer 的 T2.1 中从 Φ 中选取的任意三元组 ψ．设 $\mathbb{F}$ 为 ψ 的第一个分量，而 $\mathbb{P}^*$ 为 Elim 从 ψ 生成的 Δ 中某一多项式系统的第一个分量．那么，从 Elim 的 E2.2 中 T 用其初式和尾式的替换可以清楚地看出，或者

$$\text{level}(\mathbb{P}^*)<\text{level}(\mathbb{F}),\quad \text{或者}\quad \text{level}(\mathbb{P}^*)=\text{level}(\mathbb{F})=\ell.$$

在后一情形，关于 x_ℓ, $\mathbb{P}^{*\langle\ell\rangle}$ 中多项式的最低次数小于 $\mathbb{F}^{\langle\ell\rangle}$ 中多项式的最低次数．由于级和次数都是正整数，任意严格下降的级或最低次数构成的序列都是有限的．因此 T2 只能有有限多个循环．这就证明了 TriSer 的终止性．

正确性．我们将算法 TriSer 看作是计算一棵多枝树 $\mathcal{T}$．与该树树根相连的是三元组 $[\mathbb{P},\mathbb{Q},\emptyset]$ (见图 3)．

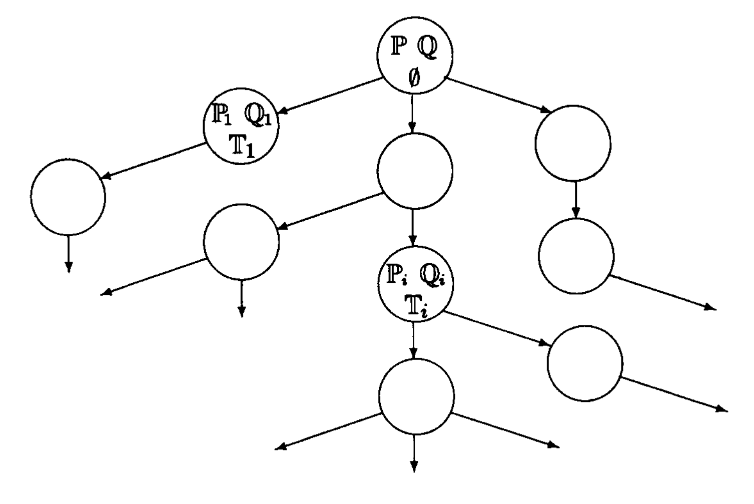


图 3　多枝分解树 $\mathcal{T}$

令 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$. 与 $\mathcal{T}$ 的每个节点或树叶 i 相连的是三元组 $[\mathbb{P}_i,\mathbb{Q}_i,\mathbb{T}_i]$, 使得在执行了 TriSer 的每步[①] 之后，零点关系

$$\mathrm{Zero}(\mathfrak{P})=\bigcup_{i\text{ 遍及 }\mathcal{T}\text{ 的所有叶点}}\mathrm{Zero}(\mathbb{P}_i\cup\mathbb{T}_i/\mathbb{Q}_i) \tag{2.3.6}$$

保持成立. 这是因为 (2.3.1) 式蕴涵着

$$\mathrm{Zero}(\mathbb{P}\cup\mathbb{T}/\mathbb{Q})=\mathrm{Zero}(\mathbb{F}\cup\{T\}\cup\mathbb{T}/\mathbb{G})\cup\bigcup_{[\mathbb{P}^*,\mathbb{Q}^*]\in\Delta}\mathrm{Zero}(\mathbb{P}^*\cup\mathbb{T}/\mathbb{Q}^*) \tag{2.3.7}$$

对任意 $\mathbb{T}$ 成立，且因为 $\mathrm{Zero}(\mathbb{F}\cup\{T\}\cup\mathbb{T}/\mathbb{G})$ 在执行步骤 P2.3 时保持不变. 很清楚，树的分支是由子算法 Elim 生成的，且使上述零点关系 (2.3.1) 因而 (2.3.7) 保持成立. 我们当然可以在任意时刻剪除 $\mathbb{P}_i$ 中含有非零常数或 $\mathbb{Q}_i$ 中含有 0 所对应的树叶 i. 如果所有树叶都因此而剪去，那么 $\mathrm{Zero}(\mathfrak{P})=\emptyset$. 否则，在算法终止时，对树 $\mathcal{T}$ 的每个叶点 i, $\mathbb{P}_i$ 都是空集. 这时，我们得到相应的 $\mathfrak{T}_i=[\mathbb{T}_i,\mathbb{U}_i]=[\mathbb{T}_i,\mathbb{Q}_i]$, 而零点分解 (2.3.6) 则形如 (2.1.7).

以下我们证明每个 $[\mathbb{T}_i,\mathbb{U}_i]$ 都是良好三角系统，即

$$\mathrm{ini}(T)(\bar{\boldsymbol{x}})\neq 0\ \text{ 对所有 } T\in\mathbb{T}_i^{\langle p\rangle},\ \bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}_i^{(p-1)}/\mathbb{U}_i)\text{ 成立},$$

且 $0\notin\mathrm{prem}(\mathbb{U}_i,\mathbb{T}_i)$. 命 $\mathbb{T}_i=[T_1,\cdots,T_r]$, 而

$$\mathrm{ini}(T_j)=I_j,\ \mathrm{cls}(T_j)=p_j,\quad j=1,\cdots,r.$$

容易看出，每个 I_j 都在 Elim 的步骤 E2.2 中被添入集合 $\mathbb{G}$. 由于 $\mathrm{cls}(I_j)<p_j$, 在对迭代 $i=p_j$ 执行了 P2.3 与 P2.4 之后 I_j 仍然留在 $\mathbb{G}$ 中. 在下一迭代 $i=p_{j-1}$ 中，I_j 将被其对 T_{j-1} 的伪余式所替代 (该伪余式不为零 —— 否则相应的叶点已被剪去). 这一伪余式将在迭代 $i=p_{j-2}$ 中进一步被其对 T_{j-2} 的非零伪余式所替代，并如此进行下去. 因而对所有 j,

$$\mathrm{prem}(I_j,\mathbb{T}_i^{\{j-1\}})=\mathrm{prem}(I_j,[T_1,\cdots,T_{j-1}])$$

都包含于 $\mathbb{U}_i$. 由伪余公式 (2.1.2) 可知，I_j 的任意零点同时又是 $\mathbb{T}_i^{\{j-1\}}$ 的零点必定也是 $\mathrm{prem}(I_j,\mathbb{T}_i^{\{j-1\}})\in\mathbb{U}_i$ 的零点. 所以，$I_j(\bar{\boldsymbol{x}})\neq 0$ 对所有 j 及 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}_i^{\{j-1\}}/\mathbb{U}_i)$ 成立.

---

① 对步骤 P2.2 与 P2.3, 多项式 T 考虑在处理中的三元组之列. 也就是说，$\mathbb{P}_i$ 对应于 $\mathbb{F}\cup\{T\}$.

由于 $\mathbb{U}_i$ 中的所有多项式实际上是某些多项式对 $\mathbb{T}_i$ 的非零伪余式，所以 $0 \notin \mathrm{prem}(\mathbb{U}_i, \mathbb{T}_i)$ 对所有 i 成立. 因而每个 $[\mathbb{T}_i, \mathbb{U}_i]$ 都是良好三角系统. 证毕.

□

算法 TriSer 实现了本节开始时所提到的由上至下、按需分裂的消元策略. 该算法结构简单而且行之有效. 注意，由 TriSer 计算的三角系统的第二个分量可能包含为数众多的多项式，这会使问题的解答 (输出) 变得复杂. 所幸的是，若所计算的良好三角系统成为正则的、简单的、或者不可约的 (见定理 3.4.6, 4.5.11 与 3.2.12)，这一弊端将不复存在.

使用 TriSer, 图 3 所示的分解树是按深度优先来计算的. 在理解了该算法的基本思想之后，读者不难设计出相应的宽度优先算法.

定义 2.3.1 由算法 PriTriSys 从 $\mathcal{K}[\boldsymbol{x}]$ 中任一多项式系统 $\mathfrak{P}$ 计算出的任意 (良好) 三角系统都称为 $\mathfrak{P}$ 的 (良好) *主三角系统*.

命题 2.3.2 设 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 而 $[\mathbb{T}, \mathbb{U}]$ 为 $[\mathbb{P}, \emptyset]$ 的主三角系统，那么 $\mathbb{T}$ 是 $\mathbb{P}$ 的拟中间列.

证 很明显，$\mathbb{T} \subset \mathrm{Ideal}(\mathbb{P})$, 且 $\mathbb{T}$ 为拟升列. 于是我们只需证明 $\mathbb{T}$ 不比 $\mathbb{P}$ 的任意拟基列 $\mathbb{B}$ 有较高的秩，即 $\mathbb{T} \precsim \mathbb{B}$. 为此，命

$$\mathbb{B} = [B_1, \cdots, B_s], \quad \mathbb{T} = [T_1, \cdots, T_r],$$

且 $p_i = \mathrm{cls}(B_i)$. 由于 $B_1 \in \mathbb{P}$ 且 $\mathrm{cls}(B_1) = p_1$, 所以 $\mathbb{P}^{\langle p_1 \rangle} \neq \emptyset$; 因此 $\mathbb{T}$ 中含有类为 p_1 的元素. 这就意味着 $\mathrm{cls}(T_1) \leq \mathrm{cls}(B_1)$. 若 $\mathrm{cls}(T_1) < \mathrm{cls}(B_1)$, 则 $\mathbb{T} \prec \mathbb{B}$; 这时命题已经获证. 否则，$\mathrm{cls}(T_1) = \mathrm{cls}(B_1)$. 从对每个 i 进行的消元过程可知，$\mathrm{ldeg}(T_1) \leq \mathrm{ldeg}(B_1)$. 所以，或者 $T_1 \prec B_1$ 或者 $T_1 \sim B_1$. 对于前者，命题已获证. 现假定后者成立.

类似地，$\mathbb{T}$ 应该含有类为 p_2 的多项式，因此有 $\mathrm{cls}(T_2) \leq \mathrm{cls}(B_2)$ 等. 使用同样的论证可知，或者存在 $j \leq \min(r, s)$, 使得

$$T_1 \sim B_1, \cdots, T_{j-1} \sim B_{j-1}, \quad 而 \quad T_j \prec B_j,$$

或者

$$s = r, \quad 且 \quad T_1 \sim B_1, \cdots, T_r \sim B_r.$$

在任一情形都有 $\mathbb{T} \precsim \mathbb{B}$, 因而命题获得证明. □

注 2.3.1 看上去，算法 TriSer 会制造大量分支. 而实际上，分支问题在这里并不比在 CharSer 中更严重. 其部分原因是，对所产生分支中的许多，相应的多项式系统都无零点. 在这种情形，多项式系统的第二个分量中有越多的多项式制造了越大的可能性来排除该系统. 一些分析表明，三角化过程所牵涉的伪除的次数在 TriSer 中与在 CharSer 中很相近. 鉴于前面所述的优点，TriSer 中单个分支的计算花费较少. 但无论如何，在具体实施时，多余分支的启发式检测总是必要和有益的.

2.4 基于子结式的算法

本节中介绍的分解算法 TriSerS 与上节的 TriSer 具有同样的功能，并且也使用分裂及由上至下的消元策略. 它们的不同之处在于 TriSerS 是基于子结式链的计算. 让我们回忆一下 1.3 节中简述的子结式理论以及多项式余式序列与子结式链之间的关系. 构造子结式链是计算多项式余式序列的最有效方法之一，这一点似乎已成定论. 在我们这里，子结式链的构造特别使得将任意多项式系统分解为 *简单系统* 成为可能 (见 3.3 节). 首先，我们说明如何将子结式链的计算作为核心运算在 TriSerS 中具体实现.

两个多项式的子结式链具有定理 1.3.4 和图 1 所示的著名块结构. 这种块结构已被柯林斯[19]、布朗、特拉布[6]、洛斯[54]与米施拉[57]等人深入研究过. 对我们来说，只使用已存在的结果而不涉及子结式理论的细节就足够了. 和前面一样，设 $\mathcal{R}$ 为一有单位元的交换环，而 $\mathcal{K}$ 是一特征为 0 的域. 对基于子结式链的分解算法，下面的引理具有特别的重要性.

引理 2.4.1 设 $S_{\mu+1}$ 和 S_μ 为 $\mathcal{R}[x]$ 中的多项式，且 $\deg(S_{\mu+1},x) \geq \deg(S_\mu,x) > 0$. 又设

$$S_{\mu+1}, S_\mu, \cdots, S_0$$

为 $S_{\mu+1}$ 和 S_μ 关于 x 的子结式链，其主子结式系数链为

$$R_{\mu+1}, R_\mu, \cdots, R_0,$$

那么对任意 $1 \leq i \leq \mu$ 有

$$S_i \neq 0, S_{i-1} = \cdots = S_0 = 0 \Longleftrightarrow R_i \neq 0, R_{i-1} = \cdots = R_0 = 0.$$

证 见 [57] 第 262 页推论 7.7.9. □

现在回顾一下定义 1.3.4 中 $S_{\mu+1}$ 和 S_μ 关于 x_k 的子结式正则子链

$$S_{d_2},\cdots,S_{d_r}.$$

我们将这些正则子结式重新命名为 $H_2,\cdots,H_r$, 且令 $P_1=S_{\mu+1}$, $P_2=S_\mu$. 显然, $H_2\backsim P_2$. 让 $\boldsymbol{x}_i$ 代表 $x_1,\cdots,x_i$ 或 $(x_1,\cdots,x_i)$, 而 $\bar{\boldsymbol{x}}_i$ 等与之类似.

引理 2.4.2 设 P_1 与 P_2 为 $\mathcal{K}[\boldsymbol{x}_k]$ 中的多项式, 且 $\deg(P_1,x_k)\geq\deg(P_2,x_k)>0$, $H_2,\cdots,H_r$ 为 P_1 和 P_2 关于 x_k 的子结式正则子链, $I=\mathrm{lc}(P_2,x_k)$, 而 $I_i=\mathrm{lc}(H_i,x_k)$, $i=2,\cdots,r$, 则

(a) 对任意 $2\leq i\leq r$ 以及 $\bar{\boldsymbol{x}}_{k-1}\in\mathrm{Zero}(\{I_{i+1},\cdots,I_r\}/II_i)$ 都有

$$\gcd(P_1(\bar{\boldsymbol{x}}_{k-1},x_k),P_2(\bar{\boldsymbol{x}}_{k-1},x_k))=H_i(\bar{\boldsymbol{x}}_{k-1},x_k).$$

(b)

$$\mathrm{Zero}(\{P_1,P_2\}/I)=\bigcup_{i=2}^{r}\mathrm{Zero}(\{H_i,I_{i+1},\cdots,I_r\}/II_i).\tag{2.4.1}$$

证　(a) 设 $\mathfrak{S}$: $S_{\mu+1},S_\mu,\cdots,S_0$ 为 $P_1=S_{\mu+1}$ 和 $P_2=S_\mu$ 关于 x_k 的子结式链, 其主子结式系数链为

$$R_{\mu+1},R_\mu,\cdots,R_0,$$

块指标为 $d_1,d_2,\cdots,d_r$, 那么 $H_i=S_{d_i}$ 以及 $I_i=R_{d_i}$ 对 $2\leq i\leq r$ 成立.

根据定义 1.3.4, 对任意 $0\leq j\leq\mu$ 而 $j\notin\{d_2,\ldots,d_r\}$, S_j 都是亏损的; 因此 R_j 恒等于零. 设

$$\bar{\boldsymbol{x}}_{k-1}\in\mathrm{Zero}(\{I_{i+1},\cdots,I_r\}/II_i),$$

则对 $0\leq j\leq d_i-1$ 有 $R_j(\bar{\boldsymbol{x}}_{k-1})=0$. 令

$$\begin{aligned}\bar{S}_j&=S_j(\bar{\boldsymbol{x}}_{k-1},x_k),\quad 0\leq j\leq\mu+1,\\ \bar{P}_i&=P_i(\bar{\boldsymbol{x}}_{k-1},x_k),\quad i=1,2,\\ \bar{H}_i&=H_i(\bar{\boldsymbol{x}}_{k-1},x_k),\quad 2\leq i\leq r.\end{aligned}\tag{2.4.2}$$

由引理 2.4.1 知

$$\bar{S}_{d_i-1}=\cdots=\bar{S}_0=0,$$

且 $\bar{H}_i=\bar{S}_{d_i}$ 是 x_k 的非零多项式. 注意, 由 $\boldsymbol{x}_{k-1}$ 到 $\bar{\boldsymbol{x}}_{k-1}$ 的特定化诱导出一同态, 该同态将 P_1 和 P_2 关于 x_k 的系数映射到 $\mathcal{K}$ 的某一扩域中的数. 依命

题 1.3.5, 每个 $\bar{S}_j$ 与 $\bar{P}_1$ 和 $\bar{P}_2$ 关于 x_k 的第 j 个子结式最多相差一个 $I(\bar{\boldsymbol{x}}_{k-1})$ $(\neq 0)$ 的幂因子. 依照子结式链块结构的定理 1.3.4, 存在整数 d, $d_i \leq d \leq \mu$, 使得 $\bar{S}_d \backsim \bar{S}_{d_i}$. 由定理 1.3.6 知, $\bar{S}_d$ 与 $\bar{P}_1$ 和 $\bar{P}_2$ 关于 x_k 的子结式多项式余式序列中的最后一个多项式相似. 所以

$$\gcd(\bar{P}_1, \bar{P}_2) = \bar{S}_d \backsim \bar{S}_{d_i} = \bar{H}_i.$$

(b) 对任意 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\emptyset/I)$, 必定存在 i $(2 \leq i \leq r)$, 使得

$$I_i(\bar{\boldsymbol{x}}_{k-1}) \neq 0, \quad I_{i+1}(\bar{\boldsymbol{x}}_{k-1}) = \cdots = I_r(\bar{\boldsymbol{x}}_{k-1}) = 0.$$

因此, 根据 (a) 有 $\bar{H}_i = \gcd(\bar{P}_1, \bar{P}_2)$, 这里 $\bar{H}_i$ 和 $\bar{P}_1, \bar{P}_2$ 如 (2.4.2) 所示. 于是欲证的零点关系立即可得. □

引理 2.4.2 (a) 可简述为: 对任意 $2 \leq i \leq r$, 在条件 $I_{i+1} = 0, \cdots, I_r = 0$ 与 $II_i \neq 0$ 之下有 $\gcd(P_1, P_2, x_k) = H_i$. 这里 $\gcd(P_1, P_2, x_k)$ 是指 P_1 和 P_2 —— 视作 x_k 的一元多项式 —— 的最大公因子. 类似的说法也将在以后的章节中用于无平方因子.

现在, 我们解释如何使用子结式链将 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P}, \mathbb{Q}]$ 分解为三角系统. 我们同样对 x_k, $k = n, \cdots, 1$, 由上至下进行消元.

若 $\mathbb{P}^{\langle k \rangle} = \emptyset$, 则消元对下一个 k 进行. 现考虑简单情形 $|\mathbb{P}^{\langle k \rangle}| = 1$, 且命 $P \in \mathbb{P}^{\langle k \rangle}$, $I = \mathrm{ini}(P)$, 那么

$$\mathbb{P} = 0, \mathbb{Q} \neq 0 \iff \begin{cases} \mathbb{P} = 0, \mathbb{Q} \neq 0, I \neq 0; \quad \text{或} \\ \mathbb{P} \setminus \{P\} = 0, I = 0, \mathrm{red}(P) = 0, \mathbb{Q} \neq 0. \end{cases}$$

这里生成了两个子系统. 对第一个子系统, 我们已经获得单个 x_k 的多项式 P, 其初式被假定为非零. 因此消元过程可对下一个 k 继续进行. 对于第二个子系统, 类为 k 的多项式关于 x_k 的极小次数已经降低. 于是按照归纳原理, 我们假定已能分解该子系统.

现在考虑一般情形 $|\mathbb{P}^{\langle k \rangle}| > 1$. 设 $P_1, P_2 \in \mathbb{P}^{\langle k \rangle}$, 其中 P_2 关于 x_k 的次数最低. 计算 P_1 和 P_2 关于 x_k 的子结式正则子链 $H_2, \cdots, H_r$. 又命 $I = \mathrm{lc}(P_2, x_k)$, 而 $I_i = \mathrm{lc}(H_i, x_k)$, $2 \leq i \leq r$ (参见引理 2.4.2), 那么

$$\mathbb{P} = 0, \mathbb{Q} \neq 0 \iff \begin{cases} \mathbb{P}_2 = 0, I = 0, \mathrm{red}(P_2) = 0, \quad \mathbb{Q} \neq 0; \quad \text{或} \\ \begin{bmatrix} \mathbb{P}_{12} = 0, H_i = 0, & \mathbb{Q} \neq 0, I \neq 0, \\ I_{i+1} = 0, \cdots, I_r = 0, & I_i \neq 0, \end{bmatrix} \\ \qquad\qquad\qquad\qquad\qquad \text{对某一 } i \ (2 \leq i \leq r), \end{cases}$$

式中

$$\mathbb{P}_2 = \mathbb{P} \setminus \{P_2\}, \quad \mathbb{P}_{12} = \mathbb{P} \setminus \{P_1, P_2\}.$$

由此可得

$$\begin{aligned}
\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) &= \mathrm{Zero}(\mathbb{P}_2 \cup \{I, \mathrm{red}(P_2)\}/\mathbb{Q}) \cup \\
&\quad \bigcup_{i=2}^{r} \mathrm{Zero}(\mathbb{P}_{12} \cup \{H_i, I_{i+1}, \cdots, I_r\}/\mathbb{Q} \cup \{I, I_i\}) \\
&= \cdots \qquad\qquad (\text{递归重复}) \\
&= \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i).
\end{aligned}$$

上述分解过程可通过下面的算法具体给出.

算法 TriSerS: $\Psi \leftarrow \mathrm{TriSerS}(\mathbb{P}, \mathbb{Q})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P}, \mathbb{Q}]$, 本算法计算 $[\mathbb{P}, \mathbb{Q}]$ 的良好三角序列 Ψ.

T1. 命 $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, n]\}$, $\Psi \leftarrow \emptyset$.

T2. 重复下列步骤直至 $\Phi = \emptyset$:

T2.1. 从 Φ 中选取三元组 $[\mathbb{T}, \mathbb{U}, \ell]$, 且命 $\Phi \leftarrow \Phi \setminus \{[\mathbb{T}, \mathbb{U}, \ell]\}$.

T2.2. 对 $k = \ell, \cdots, 1$ 执行下列步骤:

T2.2.1. 若 $\mathbb{T}^{\langle k \rangle} = \emptyset$, 则转至 T2.2.3; 否则重复下列步骤:

T2.2.1.1. 从 $\mathbb{T}^{\langle k \rangle}$ 中选取一个关于 x_k 次数最低的多项式 P_2, 且命

$$\Phi \leftarrow \Phi \cup \{[\mathbb{T} \setminus \{P_2\} \cup \{\mathrm{ini}(P_2), \mathrm{red}(P_2)\}, \mathbb{U}, k]\},$$
$$\mathbb{U} \leftarrow \mathbb{U} \cup \{\mathrm{ini}(P_2)\}.$$

若 $|\mathbb{T}^{\langle k \rangle}| = 1$, 则转至 T2.2.2. 否则, 从 $\mathbb{T}^{\langle k \rangle} \setminus \{P_2\}$ 中任选多项式 P_1.

T2.2.1.2. 计算 P_1 和 P_2 关于 x_k 的子结式正则子链 $H_2, \cdots, H_r$, 且命 $I_i \leftarrow \mathrm{lc}(H_i, x_k)$, $2 \le i \le r$. 若 $\mathrm{cls}(H_r) < k$, 则命 $\bar{r} \leftarrow r - 1$; 否则命 $\bar{r} \leftarrow r$.

T2.2.1.3. 命

$$\begin{aligned}
\Phi &\leftarrow \Phi \cup \{[\mathbb{T} \setminus \{P_1, P_2\} \cup \{H_i, I_{i+1}, \cdots, I_r\}, \\
&\qquad\qquad \mathbb{U} \cup \{I_i\}, k]\colon\ 2 \le i \le \bar{r} - 1\}, \\
\mathbb{T} &\leftarrow \mathbb{T} \setminus \{P_1, P_2\} \cup \{H_r, H_{\bar{r}}\}, \\
\mathbb{U} &\leftarrow \mathbb{U} \cup \{I_{\bar{r}}\}.
\end{aligned}$$

T2.2.2. 计算 $\mathbb{U} \leftarrow \operatorname{prem}(\mathbb{U}, P_2)$.

T2.2.3. 若 $\mathbb{T} \cap \mathcal{K} \setminus \{0\} \neq \emptyset$ 或 $0 \in \mathbb{U}$, 则回到 T2.

T2.3. 命 $\Psi \leftarrow \Psi \cup \{[\mathbb{T}, \mathbb{U}]\}$, 并将 $\mathbb{T}$ 排 (序) 成三角列.

证 该算法采用了从 x_n 到 x_1 的由上至下消元过程. 对每个 x_k, 只要 $\mathbb{T}^{\langle k\rangle} \neq \emptyset$ (步骤 T2.2.1), 就首先对 $\mathbb{T}^{\langle k\rangle}$ 中的多项式进行消元, 生成单个类为 k 的多项式 P_2; 该多项式然后用来约化 $\mathbb{U}$ 中的多项式 (步骤 T2.2.2). 算法中有两种分裂. 其一是在 T2.2.1.1 中按所考虑的多项式的初式是否为零来进行的: 或者假定该初式不为零, 或者所考虑的多项式被其初式和尾式来替换. 另一种分裂是在步骤 T2.2.1.3 中按引理 2.4.2 用子结式正则子链消元来进行的. 每次分裂时, 生成的系统之一 (相当于引理 2.4.2 (b) 中的情形 $i = r$ 或 $r - 1$) 用来更新当前的系统 $[\mathbb{T}, \mathbb{U}]$, 其他生成的系统则全部添入 Φ. 由于在将多项式系统 $\mathfrak{P}$ 分裂为子系统 $\mathfrak{P}_i$ 的每种情形, 零点关系

$$\operatorname{Zero}(\mathfrak{P}) = \bigcup_i \operatorname{Zero}(\mathfrak{P}_i)$$

都保持成立, 所以我们最终得到零点分解 (2.1.7). 鉴于步骤 T2.2.2 和 T2.2.3, 每个求得的三角系统作为 (2.1.7) 中的 $\mathfrak{T}_i$ 都是良好的.

算法的终止性是有保证的, 其原因是在分裂的每种情形, 新多项式系统都是从当前系统按两种方式产生的: 或者用一个次数较低的多项式来替换一个 (关于它们的公共导元) 次数较高的多项式, 或者用一个多项式来替换两个类同为 k 的多项式. 对于后一种情形, 可能会添入一些类小于 k 的多项式. 在 T2.2.1 的每次重复中, 都是两个多项式 $P_1, P_2 \in \mathbb{T}^{\langle k\rangle}$ 被一个类为 k 的 $H_{\bar{r}}$ —— 有时加上一个类 $< k$ 的多项式 H_r —— 所替代 (见 T2.2.1.3). 所以该步骤明显终止. □

下例中的多项式组见诸于 [100, 25, 88], 它源自布朗斯坦的一篇论文.

例 2.4.1 设 $\mathbb{P} = \{P_1, P_2, P_3\}$, 其中

$$\begin{aligned} P_1 &= x^2 + y^2 + z^2 - r^2, \\ P_2 &= xy + z^2 - 1, \\ P_3 &= xyz - x^2 - y^2 - z + 1, \end{aligned}$$

而 $r \prec z \prec x \prec y$.

首先假定 $\mathrm{ini}(P_2)=x\neq 0$, 并分别计算 P_3,P_2 以及 P_1,P_2 关于 y 的子结式链. 我们得到 P_3,P_2,F 与 P_1,P_2,G, 其中

$$F=-x^4-z^3x^2+x^2-z^4+2z^2-1,$$
$$G=x^4+z^2x^2-r^2x^2+z^4-2z^2+1.$$

因此 P_2,F 与 P_2,G 分别为 P_3,P_2 与 P_1,P_2 的子结式正则子链. 故在 $F=G=0$ 且 $x\neq 0$ 时有

$$\gcd(P_3,P_2,y)=\gcd(P_1,P_2,y)=P_2.$$

从例 1.3.2 中求得的 F 和 G 的子结式链可以看出, F 和 G 关于 x 的子结式正则子链为

$$G,\quad H^2x^2,\quad (z^4-2z^2+1)^2H^4,$$

其中 $H=z^3-z^2+r^2-1$. 所以

$$\gcd(F,G,x)=\begin{cases} G & \text{若 } H=0,\\ x^2 & \text{若 } z^4-2z^2+1=0, H\neq 0.\end{cases}$$

由于假定 x 非零, 后一情形已被排除在外. 因而我们获得一个良好的三角系统 $[\mathbb{T}_1,\mathbb{U}_1]$, 其中

$$\mathbb{T}_1=[H,G,P_2],\quad \mathbb{U}_1=\{x\}.$$

至于 $x=0$ 的情形, 通过用 $\mathrm{ini}(P_2)=x$ 和 $\mathrm{red}(P_2)=z^2-1$ 来替换 P_2 可得一新的多项式组. 遵循同样的程序, 可从该多项式组求得第二个三角系统 $[\mathbb{T}_2,\emptyset]$, 其中

$$\mathbb{T}_2=[r^4-4r^2+3,z+r^2-2,x,y^2-r^2+1].$$

由此即得

$$\mathrm{Zero}(\mathbb{P})=\mathrm{Zero}(\mathbb{T}_1/x)\cup\mathrm{Zero}(\mathbb{T}_2).$$

例 2.4.2 使用 TriSerS, 例 2.3.1 中的多项式组 $\mathbb{P}$ 可分解为下列约化三角系统:

$$\mathfrak{T}_1=[[-z^5+t^4,T_2,T_3],\{t(t^3-1),z\}],$$
$$\mathfrak{T}_2=[[t,z,y,x],\emptyset],$$
$$\mathfrak{T}_3=[[t(t^3-1),-z^5+t,tzy^2+2z^3y+1,zx^2-t],\{z\}],$$

其中

$$T_2=-tzy^2-2z^3y+t^8-2t^5-t^3+t^2,\quad T_3=t^4x-tx-ty-z^2,$$

使得

$$\operatorname{Zero}(\mathbb{P}) = \bigcup_{i=1}^{3} \operatorname{Zero}(\mathfrak{T}_i).$$

为方便读者将 $\mathfrak{T}_1$ 中的三角列与例 2.3.2 中的 $\mathbb{T}_1 = [R_3, R_5, R_4]$ 作比较，我们顺便指出

$$t^3 T_2 = \operatorname{prem}(R_5, R_3, z), \quad -t^3 T_3 = \operatorname{prem}(z^2 R_4, R_3, z).$$

例 2.4.3 设 $\mathbb{P} = \{P_1, P_2, P_3\}$, 其中

$$\begin{aligned} P_1 &= z\,(x^2 + y^2 - c) + 1, \\ P_2 &= y\,(x^2 + z^2 - c) + 1, \\ P_3 &= x\,(y^2 + z^2 - c) + 1. \end{aligned}$$

这组多项式选自诺恩堡的一篇论著；文献 [25, 88] 中对其也有讨论. 在变元序 $c \prec z \prec y \prec x$ 之下，用 TriSerS 可将 $\mathbb{P}$ 分解为 7 个良好三角系统 $[\mathbb{T}_1, \mathbb{U}_1], \cdots, [\mathbb{T}_7, \mathbb{U}_7]$, 使得

$$\operatorname{Zero}(\mathbb{P}) = \bigcup_{i=1}^{7} \operatorname{Zero}(\mathbb{T}_i/\mathbb{U}_i),$$

其中

$$\begin{aligned}
\mathbb{T}_1 &= [2\,cz^4 - 2\,z^3 - c^2z^2 - 2\,cz - 1, (cz+1)\,y + cz^2 - z, 2\,z^2x + cz + 1], \\
\mathbb{T}_2 &= [2\,z^4 - 3\,cz^2 + z + c^2, zy - z^2 + c, x - z], \\
\mathbb{T}_3 &= [z^3 - cz - 1, (z^2 - c)\,y^2 + y - cz^2 + z + c^2, yx - z^2 + c], \\
\mathbb{T}_4 &= [2\,z^4 - 3\,cz^2 + z + c^2, (2\,z^3 - 2\,cz + 2)\,y - cz^2 - z + c^2, P_3], \\
\mathbb{T}_5 &= [2\,z^3 - cz + 1, y - z, 2\,z^2x - cx + 1], \\
\mathbb{T}_6 &= [c, 2\,z^3 + 1, y - z, 2\,z^2x + 1], \\
\mathbb{T}_7 &= [4\,c^3 - 27, 9\,z + 2\,c^2, 6\,cy^2 - 9\,y - 4\,c^2, 3\,yx + 2\,c]; \\
\mathbb{U}_1 &= \{c, z, cz + 1\}, \\
\mathbb{U}_2 &= \{z, z^2 - c, 2\,z^2 - c\}, \\
\mathbb{U}_3 &= \{z^2 - c, y\}, \\
\mathbb{U}_4 &= \{z^2 - c, z^3 - cz + 1, z^3 - cz - 1\}, \\
\mathbb{U}_5 &= \{z, 2\,z^2 - c\}, \\
\mathbb{U}_6 &= \{z\}, \\
\mathbb{U}_7 &= \{c, y\}.
\end{aligned}$$

在计算这些三角系统时，某些中间多项式在 Q 上被分解为不可约因子. 参见注 2.4.2.

算法 TriSer 和 TriSerS 中使用的两种数据结构稍有差异. 这样做主要是遵循我们算法设计的早期思路并用以说明这两种可能性. 将算法之一的数据结构用于另一算法也是可以的.

注 2.4.1 关于 TriSer 和 TriSerS 的实施，一些技术性的细节需要考虑在内以便提高效率. 譬如，一旦 $\mathbb{P}$ 中出现非零常数或者 $0 \in \mathbb{Q}$, 即知多项式系统 $[\mathbb{P}, \mathbb{Q}]$ 无零点. $\mathbb{P}$ 中多项式的任一因子，要是作为因子出现在 $\mathbb{Q}$ 的某一多项式中，应立即抹去；这样的因子也可从 $\mathbb{Q}$ 的其他多项式中抹去. 用某些多项式去约化和化简其他多项式的策略应该被启发式地使用. 通常的求最大公因子和无平方因子分解可与条件最大公因子和无平方因子的计算一起混合使用. 下面是一个更特殊的小技巧：对任意 $[\mathbb{P}, \mathbb{Q}]$, 若 $|\mathbb{P}^{\langle 1 \rangle}| \geq 2$, 则 $\text{Zero}(\mathbb{P}/\mathbb{Q})$ 很可能是空集；是否确实如此可以通过先计算 $\mathbb{P}^{\langle 1 \rangle}$ 中多项式的最大公因子来加以验证.

注 2.4.2 为了减少用 CharSer, TriSer 或 TriSerS 计算三角序列的花费，可以在适当的时候启发式地对某些中间多项式进行因子分解以将多项式系统分裂. 如果多项式组 $\mathbb{P}$ 中的某个多项式被分解成，比如说，两个多项式的乘积，因而 $[\mathbb{P}, \mathbb{Q}]$ 可被分裂为两个多项式系统，设为 $[\mathbb{P}', \mathbb{Q}]$ 和 $[\mathbb{P}'', \mathbb{Q}]$, 使得

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \text{Zero}(\mathbb{P}'/\mathbb{Q}) \cup \text{Zero}(\mathbb{P}''/\mathbb{Q}),$$

那么我们可以对 $[\mathbb{P}', \mathbb{Q}]$ 和 $[\mathbb{P}'', \mathbb{Q}]$ 分别进行分解，而不必去分解 $[\mathbb{P}, \mathbb{Q}]$. 一般来说，多项式因子分解是费时的，但对其适当运用可以提高分解算法的效率. 我们将在第四章中对这一问题作更加细致的处理.

我们在前几节中已经看到，计算分解 (2.1.7) 的程序并不复杂. 然而，所得的良好三角系统仍会有 “不良行为”，因此我们将在以后的章节中引进复杂得多的算法，以便计算各种具有良好行为的三角系统.

第三章　正则系统与简单系统

由算法 CharSer, TriSer 和 TriSerS 求得的良好三角系统不一定是*完美的*. 换句话说，那些无零点的三角系统并不一定被排除在外. 这一问题将是本章和下一章研究的对象. 为了获得一些初步的想法，让我们先看下面的例子.

例 3.1　考虑良好三角列 $\mathbb{T} = [T_1, T_2, T_3]$, 其中

$$\begin{aligned} T_1 &= x^2 + u, \\ T_2 &= y^2 + 2\,xy - u, \\ T_3 &= (x + y)\,z + 1, \end{aligned}$$

而 $u \prec x \prec y \prec z$. 这时 $I = \mathrm{ini}(T_3) = x + y$. 我们想检验 $\mathrm{Zero}(\mathbb{T}) = \emptyset$ 是否成立. 对此有四种不同的办法可供使用.

因子分解. 为了理解 $\mathbb{T}$ 的“不良行为”, 我们先注意 T_2 在 $\mathbb{Q}(u, x)$ 上的因子分解

$$T_2 \doteq (y + x)^2 = I^2,$$

这里 T_1 是 x 的添加多项式. 于是很明显，三角列 $\mathbb{T}$ 无零点.

投影. 不用代数因子分解，我们计算

$$\mathrm{prem}(I^2, T_2) = x^2 + u = T_1,$$

这里 $\deg(T_2, y) = 2$ 取为 I 的幂次. 由此可得同样结论.

无平方因子分解. 作为另一途径，我们考虑

$$\mathrm{prem}(T_2, \partial T_2/\partial y) = -4\,(x^2 + u) = -4\,T_1.$$

这说明, 在 $T_1 = 0$ 时 T_2 是某个多项式 T 的平方. 很容易确定 T 为 $I = y + x$. 因此，我们也可以作出 $\mathbb{T}$ 无零点的结论.

计算最大公因子. 最后，我们计算

$$\mathrm{prem}(T_2, I_2) = -(x^2 + u) = -T_1.$$

由此可知，在 $T_1 = 0$ 时 I 是 T_2 和 I 的最大公因子. 所以 $\mathrm{Zero}(\mathbb{T}) = \emptyset$ 同样得到验证.

下面的目的是将以上技巧发展成为系统的算法. 我们首先介绍正则系统和简单系统及其计算. 对此, 子结式正则子链将担任重要角色. 无零点三角系统也可以通过将 *投影* 运算并入某些算法来加以排除. 如果实现了不可约分解, 三角系统的完美性也会得到保证. 这些将是第四章的主题.

3.1 分解为正则系统

我们想对第二章中所描述的基于子结式的算法作适当修改, 以便将任意多项式系统分解为正则系统.

定义 3.1.1 $\mathcal{K}[\boldsymbol{x}]$ 中的三角系统 $[\mathbb{T},\mathbb{U}]$ 称为是 *正则的* 或 *正则系统*, 如果对任意 $1 \leq k \leq n$:

(a) 或者 $\mathbb{T}^{\langle k\rangle} = \emptyset$, 或者 $\mathbb{U}^{\langle k\rangle} = \emptyset$;

(b) 对任意 $I \in \mathrm{ini}(\mathbb{U}^{\langle k\rangle})$ 及 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\mathbb{T}^{(k-1)}/\mathbb{U}^{(k-1)})$ 都有

$$I(\bar{\boldsymbol{x}}_{k-1}) \neq 0.$$

三角列 $\mathbb{T}$ 称为是 *正则的* 或 *正则列*, 如果存在多项式组 $\mathbb{U}$, 使得 $[\mathbb{T},\mathbb{U}]$ 是正则系统.

称三角序列 Ψ 为 *正则序列*, 如果每个 $\mathfrak{T} \in \Psi$ 都是正则系统.

称 Ψ 为多项式系统 $\mathfrak{P}$ 的 *正则序列*, 如果它是正则序列, 且

$$\mathrm{Zero}(\mathfrak{P}) = \bigcup_{\mathfrak{T}\in\Psi} \mathrm{Zero}(\mathfrak{T}). \tag{3.1.1}$$

$[\mathbb{P},\emptyset]$ 的正则序列也被称为多项式组 $\mathbb{P}$ 的 *正则序列*.

在上面的定义中, 因为 $[\mathbb{T},\mathbb{U}]$ 是三角系统, 条件 (b) 对每个 $I \in \mathrm{ini}(\mathbb{T}^{\langle k\rangle})$ 也是满足的.

例如, 对变元序 $x \prec y$, 由于 $[[xy-1],\{x\}]$ 是正则系统, 所以 $[xy-1]$ 是正则列; 但 $\mathbb{T} = [x^2-1,(x+1)y-1]$ 却不是. 其原因是, 依据定义 $[\mathbb{T},\emptyset]$ 不是三角系统, 而 $\mathbb{U} = \emptyset$ 是仅有的可能的集合, 使得条件 (a) 成立.

为方便起见, 有时也将 $\emptyset$ 视作正则列.

引理 3.1.1 设 P_1 和 P_2 为 $\mathcal{K}[\boldsymbol{x}_k]$ 中满足 $\deg(P_1,x_k) \geq \deg(P_2,x_k) > 0$ 的多项式, $H_2,\cdots,H_r$ 为 P_1 和 P_2 关于 x_k 的子结式正则子链, 而

$$I = \mathrm{lc}(P_2,x_k),\quad I_i = \mathrm{lc}(H_i,x_k),\quad 2 \leq i \leq r.$$

又设 $\mathbb{P},\mathbb{Q}$ 为 $\mathcal{K}[\boldsymbol{x}_{k-1}]$ 中的多项式组，并假定对任意 $\bar{\boldsymbol{x}}_{k-1}\in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 有 $I(\bar{\boldsymbol{x}}_{k-1})\neq 0$, 那么

$$\mathrm{Zero}(\mathbb{P}\cup\{P_2\}/\mathbb{Q}\cup\{P_1\})=\bigcup_{i=2}^{r}\mathrm{Zero}(\mathbb{P}\cup\mathbb{P}_i/\mathbb{Q}\cup\{P_1,I_i\}),\tag{3.1.2}$$

其中 $\mathbb{P}_i=\{\mathrm{pquo}(P_2,H_i,x_k),I_{i+1},\cdots,I_r\}$, $2\leq i\leq r$. 若 $\mathrm{cls}(H_r)<k$, 则 $I_r=H_r$, 且

$$\mathrm{Zero}(\mathbb{P}\cup\mathbb{P}_r/\mathbb{Q}\cup\{P_1,I_r\})=\mathrm{Zero}(\mathbb{P}\cup\{P_2\}/\mathbb{Q}\cup\{I_r\}).\tag{3.1.3}$$

证 对任意 $\bar{\boldsymbol{x}}_{k-1}\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$, 一定存在某个 i $(2\leq i\leq r)$, 使得

$$I_i(\bar{\boldsymbol{x}}_{k-1})\neq 0,\quad I_{i+1}(\bar{\boldsymbol{x}}_{k-1})=\cdots=I_r(\bar{\boldsymbol{x}}_{k-1})=0.\tag{3.1.4}$$

按照引理 2.4.2 (a), 我们有

$$H_i(\bar{\boldsymbol{x}}_{k-1},x_k)=\gcd(P_1(\bar{\boldsymbol{x}}_{k-1},x_k),P_2(\bar{\boldsymbol{x}}_{k-1},x_k)).\tag{3.1.5}$$

由此即得零点关系 (3.1.2).

在 $\mathrm{cls}(H_r)<k$ 时显然有 $I_r=H_r$, 而 $\mathbb{P}_r=\{P_2\}$. 如果 $I_r(\bar{\boldsymbol{x}}_{k-1})=0$, (3.1.3) 式的两边都为空集. 否则

$$\gcd(P_1(\bar{\boldsymbol{x}}_{k-1},x_k),P_2(\bar{\boldsymbol{x}}_{k-1},x_k))=I_r(\bar{\boldsymbol{x}}_{k-1})\neq 0.$$

于是

$$\mathrm{Zero}(\mathbb{P}\cup\{P_2\}/\mathbb{Q}\cup\{P_1,I_r\})=\mathrm{Zero}(\mathbb{P}\cup\{P_2\}/\mathbb{Q}\cup\{I_r\}),$$

因而 (3.1.3) 成立. □

分解 (3.1.2) 的意义在于：$\mathbb{P}_i$ 中的多项式 $\mathrm{pquo}(P_2,H_i,x_k)$, 除 $i=r$ 且 $\mathrm{cls}(H_r)<k$ 外，总比 P_2 关于 x_k 有较低的次数. 而在 $\mathrm{cls}(H_r)<k$ 时，多项式 P_1 可按 (3.1.3) 抹去.

下面的算法 RegSer 是 TriSer 的扩展；也可视其为从 (3.3 节中的) SimSer 简化而得. 该算法将任意多项式系统分解为有限多个正则系统，它关于等式多项式的消元策略与 TriSer 中所使用的几乎完全一样. 主要的新成分是步骤 R2.2.3: 步骤 R2.2.2 中得到的类为 k 的多项式 P_2 被用来消去 $\mathbb{U}^{\langle k\rangle}\neq\emptyset$ 中的非等式多项式. 粗略地说，这一消去过程是通过计算子结式正则子链并按照 (3.1.2) 重复使用 pquo 将 P_2 和 P_1 的条件最大公因子 H_i 从 P_2 中抹去；最终在无这样的公因子可抹时，则按 (3.1.3) 将 P_1 消去.

算法 RegSer: $\Psi\leftarrow\mathrm{RegSer}(\mathbb{P},\mathbb{Q})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P},\mathbb{Q}]$, 本算法计算 $[\mathbb{P},\mathbb{Q}]$ 的正则序列 Ψ.

R1. 命 $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, n]\}, \Psi \leftarrow \emptyset$.

R2. 重复下列步骤直至 $\Phi = \emptyset$:

R2.1. 从 Φ 中选取元素 $[\mathbb{T}, \mathbb{U}, l]$, 且命 $\Phi \leftarrow \Phi \setminus \{[\mathbb{T}, \mathbb{U}, l]\}$.

R2.2. 对 $k = l, \cdots, 1$ 执行下列步骤:

R2.2.1. 命 $\mathbb{T} \leftarrow \mathbb{T} \setminus \{0\}, \mathbb{U} \leftarrow \mathbb{U} \setminus (\mathcal{K} \setminus \{0\})$. 如果 $\mathbb{T} \cap \mathcal{K} \neq \emptyset$ 或 $0 \in \mathbb{U}$, 则转回 R2. 若 $\mathbb{T}^{\langle k \rangle} = \emptyset$, 则转至 R2.2.4.

R2.2.2. 重复下列步骤:

R2.2.2.1. 设 P_2 为 $\mathbb{T}^{\langle k \rangle}$ 中关于 x_k 次数最低的多项式. 命

$$\begin{aligned}&\Phi \leftarrow \Phi \cup \{[\mathbb{T} \setminus \{P_2\} \cup \{\mathrm{ini}(P_2), \mathrm{red}(P_2)\}, \mathbb{U}, k]\},\\ &\mathbb{U} \leftarrow \mathbb{U} \cup \{\mathrm{ini}(P_2)\}.\end{aligned}$$

若 $|\mathbb{T}^{\langle k \rangle}| = 1$, 则转至 R2.2.3; 否则从 $\mathbb{T}^{\langle k \rangle} \setminus \{P_2\}$ 中选取多项式 P_1.

R2.2.2.2. 计算 P_1 和 P_2 关于 x_k 的子结式正则子链 $H_2, \cdots, H_r$, 且对 $2 \leq i \leq r$ 命 $I_i \leftarrow \mathrm{lc}(H_i, x_k)$. 如果 $\mathrm{cls}(H_r) < k$, 则命 $\bar{r} \leftarrow r - 1$; 否则命 $\bar{r} \leftarrow r$.

R2.2.2.3. 命

$$\begin{aligned}&\Phi \leftarrow \Phi \cup \{[\mathbb{T} \setminus \{P_1, P_2\} \cup \{H_i, I_{i+1}, \cdots, I_r\},\\ &\qquad\qquad \mathbb{U} \cup \{I_i\}, k]:\ 2 \leq i \leq \bar{r} - 1\},\\ &\mathbb{T} \leftarrow \mathbb{T} \setminus \{P_1, P_2\} \cup \{H_r, H_{\bar{r}}\},\\ &\mathbb{U} \leftarrow \mathbb{U} \cup \{I_{\bar{r}}\}.\end{aligned}$$

R2.2.3. 重复下列步骤直至 $\mathbb{U}^{\langle k \rangle} = \emptyset$ 或 $\mathrm{cls}(P_2) < k$:

R2.2.3.1. 设 P_1 为 $\mathbb{U}^{\langle k \rangle}$ 中的多项式; 若 $\deg(P_1, x_k) \geq \deg(P_2, x_k)$, 则计算 P_1 和 P_2 —— 否则计算 P_2 和 P_1 —— 关于 x_k 的子结式正则子链 $H_2, \cdots, H_r$, 且对 $2 \leq i \leq r$ 命 $I_i \leftarrow \mathrm{lc}(H_i, x_k)$.

R2.2.3.2. 命

$$\begin{aligned}&\Phi \leftarrow \Phi \cup \{[\mathbb{T} \setminus \{P_2\} \cup \{\mathrm{pquo}(P_2, H_i, x_k), I_{i+1}, \cdots, I_r\},\\ &\qquad\qquad \mathbb{U} \cup \{I_i\}, k]:\ 2 \leq i \leq r - 1\},\\ &\mathbb{T} \leftarrow \mathbb{T} \setminus \{P_2\} \cup \{\mathrm{pquo}(P_2, H_r, x_k)\},\\ &P_2 \leftarrow \mathrm{pquo}(P_2, H_r, x_k).\end{aligned}$$

如果 $\mathrm{cls}(H_r) < k$, 则命 $\mathbb{U} \leftarrow \mathbb{U} \setminus \{P_1\} \cup \{I_r\}$; 否则命 $\mathbb{U} \leftarrow \mathbb{U} \cup \{I_r\}$.

R2.2.4. 若 $\mathbb{U}^{\langle k\rangle} \neq \emptyset$, 则对每个 $P_1 \in \mathbb{U}^{\langle k\rangle}$ 命

$$\Phi \leftarrow \Phi \cup \{[\mathbb{T} \cup \{\mathrm{ini}(P_1)\}, \mathbb{U} \setminus \{P_1\} \cup \{\mathrm{red}(P_1)\}, k]\},$$
$$\mathbb{U} \leftarrow \mathbb{U} \cup \{\mathrm{ini}(P_1)\}.$$

R2.3. 命 $\Psi \leftarrow \Psi \cup \{[\mathbb{T}, \mathbb{U}]\}$, 其中 $\mathbb{T}$ 排为三角列.

证 *正确性.* 我们首先注意, 在 $\deg(P_1, x_k) < \deg(P_2, x_k)$ 时, 步骤 R2.2.3.1 中 P_1 和 P_2 的互换不会引起任何问题. 为了说明这一点, 我们断言, 在将 I 设为 $\mathrm{lc}(P_1, x_k)$ 而不是 $\mathrm{lc}(P_2, x_k)$ 时, 引理 2.4.2 (a) 仍然成立. 需要考虑导系数 I (如该引理的证明所示) 的原因是, 在 P_1 和 P_2 关于 x_k 的系数被特定化时, 子结式之间可以相差一个 I 的若干次幂的因子. 按照命题 1.3.5, P_1 和 P_2 的哪个导系数被取作 I 并被假定不为零是无关紧要的. 因而, 引理 3.3.2 中的 (3.3.1) 式在 $\deg(P_1, x_k) < \deg(P_2, x_k)$ 而 $H_2, \cdots, H_r$ 为 P_2 和 P_1 关于 x_k 的子结式正则子链 (但 I 保持不变) 时仍然成立. [可能发生的情形: 对某个 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\emptyset/I)$ (参阅引理 3.3.2 的证明) 有

$$I_2(\bar{\boldsymbol{x}}_{k-1}) = \cdots = I_r(\bar{\boldsymbol{x}}_{k-1}) = 0.$$

此时 $P_1(\bar{\boldsymbol{x}}_{k-1}, x_k) \equiv 0$, 因而 $\mathrm{Zero}(P_2/P_1 I) = \emptyset$. 所以, 这一情形不必考虑.]

现在我们留意, 在 RegSer 的每种分裂情形, 都是一个分裂的系统被用来更新当前系统 $[\mathbb{T}, \tilde{\mathbb{T}}]$; 该系统对应于 (2.4.1) 和 (3.1.2) 中 $i = r$ 的情形, 但有一个例外: 在 $\mathrm{cls}(H_r) < k$ 时, 它对应于 (2.4.1) 中 $i = r - 1$ 的情形. 其他分裂的系统则被添入 Φ. 依据 (2.4.1), (3.1.2), (3.1.3) 以及关于第一类分裂的明显零点关系 (2.3.1), 以下形式的零点分解总是成立的:

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{\alpha} \mathrm{Zero}(\mathbb{P}_\alpha/\mathbb{Q}_\alpha), \tag{3.1.6}$$

这里求并是对所有分裂的系统. 因而, 我们最终将获得分解 (3.1.1), 其中 $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$. 根据定义, 所计算出的 Ψ 中的有序多项式组的对都是正则系统.

终止性. 首先注意, 步骤 R2.2.2 和 R2.2.3 显然终止; 这是由于在 R2.2.2 的每个循环中都是两个多项式 $P_1, P_2 \in \mathbb{T}^{\langle k\rangle}$ 由一个类为 k 的多项式 $H_{\bar{r}}$ 所替代 (见 R2.2.2.3), 而在 R2.2.3 的每个循环中或者一个多项式 P_2 被关于 x_k 次数较低的 $\mathrm{pquo}(P_2, H_r, x_k)$ 所替代, 或者一个多项式 $P_1 \in \tilde{\mathbb{T}}^{\langle k\rangle}$ 被删除 (见 R2.2.3.2). 在每种分裂情形, 分裂了的多项式系统都是从当前系统通过两种

方式获得的：或者用一个关于其公共导元 x_k 有较低次数的多项式去替换一个或两个多项式 (大多数情形)，或者抹去一个类为 k 的多项式 (如 R2.2.2.3 中 $\bar{r}=2$ 和 R2.2.3.2 中 $i=r$ 且 $\operatorname{cls}(H_r)<k$ 的情形)，但有时候有类 $<k$ 的多项式被添加进去．由此可见，循环 R2 只可能重复有限多次． □

例 3.1.1 用 RegSer 可将例 2.4.1 中的多项式组 $\mathbb{P}$ 分解为 4 个正则系统 $[\mathbb{T}_i,\mathbb{U}_i]$，使得

$$\operatorname{Zero}(\mathbb{P})=\bigcup_{i=1}^{4}\operatorname{Zero}(\mathbb{T}_i/\mathbb{U}_i),$$

其中

$$\begin{aligned}\mathbb{T}_3&=[r^4-4r^2+3,-z^2+r^2z-z-r^2+1,F,P_2],\\ \mathbb{U}_1&=\{r^4-4r^2+3\},\quad \mathbb{U}_2=\mathbb{U}_3=\mathbb{U}_4=\emptyset,\end{aligned}$$

$\mathbb{T}_1,\mathbb{T}_2$ 以及 F,P_2 与例 2.4.1 中相同，而 $\mathbb{T}_4$ 如例 3.3.4 所示.

为说明其细节，我们用 T_1,T_2,T_3 依次表示 $\mathbb{T}_1$ 中的三个多项式．计算 $\operatorname{ini}(T_3)=x$ 和 T_2 关于 x 的子结式正则子链；设 R 为该子链中的最后一个多项式 (它与 x 和 T_2 关于 x 的结式相等)．$\mathbb{U}_1$ 中的非等式多项式是 R (抹去其因子方幂之后) 和 T_1 关于 z 的子结式正则子链中的最后一个多项式．在按照子结式正则子链进行分裂时会产生一些新的多项式系统，由此而获得正则列 $\mathbb{T}_3$ 和 $\mathbb{T}_4$.

例 3.1.2 考虑 $\mathbb{P}=\{P_1,\cdots,P_4\}$，其中

$$\begin{aligned}P_1&=(x-u)^2+(y-v)^2-1,\\ P_2&=v^2-u^3,\\ P_3&=2v(x-u)+3u^2(y-v),\\ P_4&=(3wu^2-1)(2wv-1).\end{aligned}$$

这组多项式由美国珀渡大学计算机科学系的弗米尔于 1990 年 4 月告诉笔者．它曾作为例子在 [81] 等文献中用来测试算法.

在变元序 $x\prec y\prec u\prec v\prec w$ 之下，由 RegSer 求得的 $\mathbb{P}$ 的正则序列含有 6 个正则系统 $[\mathbb{T}_1,\mathbb{U}_1],[\mathbb{T}_2,\emptyset],\cdots,[\mathbb{T}_6,\emptyset]$，其中

$$\begin{aligned}\mathbb{T}_1&=[T_{11},T_{12},P_3,P_4], &\mathbb{T}_2&=[T_{31},T_{22},T_{12},P_3,P_4],\\ \mathbb{T}_3&=[T_{31},T_{32},T_{33},P_3,P_4], &\mathbb{T}_4&=[T_{41},T_{42},T_{43},P_3,P_4],\end{aligned}$$

$$\begin{aligned}\mathbb{T}_5&=[T_{41},y,12xu+2u-9x^2-2x+9,v^2+u^2-2xu+x^2-1,P_4],\\ \mathbb{T}_6&=[x,729y^4-956y^2-529,85u-81y^2+72,\\ &\qquad 6y^2v+23v+12y^3-39y,P_4],\end{aligned}$$

其中

$$
\begin{aligned}
T_{11} &= 729\,y^6 - Hy^4 + (729\,x^6 - 1458\,x^5 - 2619\,x^4 - 4892\,x^3 - 297\,x^2 \\
&\quad + 5814\,x + 427)\,y^2 + 729\,x^8 + 216\,x^7 - 2900\,x^6 - 2376\,x^5 + 3870\,x^4 \\
&\quad + 4072\,x^3 - 1188\,x^2 - 1656\,x + 529, \\
T_{12} &= [2187\,y^4 - 6\,(729\,x^3 + 162\,x^2 + 2079\,x + 478)\,y^2 + 2187\,x^6 - 1944\,x^5 \\
&\quad - 10125\,x^4 - 4800\,x^3 + 2501\,x^2 + 4968\,x - 1587]\,u + 4\,x^2 G, \\
T_{22} &= 729\,(30618\,x^5 + 38151\,x^4 + 8316\,x^3 + 2286\,x^2 + 59092\,x + 20664)\,y^2 \\
&\quad + 279686682\,x^5 - 194912487\,x^4 + 343568520\,x^3 + 126051867\,x^2 \\
&\quad + 74246894\,x + 30796164, \\
T_{31} &= (81x^2 + 18x + 28)\,(729x^4 + 972x^3 - 1026x^2 + 1684x + 765), \\
T_{32} &= 6\,(18\,x - 1)\,(81\,x^2 + 81\,x + 83)\,y^2 - 2187\,x^6 + 7776\,x^5 + 18252\,x^4 \\
&\quad - 4812\,x^3 - 4787\,x^2 + 540\,x + 2766, \\
T_{33} &= (243\,x^2 + 36\,x + 85)\,u^2 - F, \\
T_{41} &= 27\,x^4 + 4\,x^3 - 54\,x^2 - 36\,x + 23, \\
T_{42} &= 19683\,y^4 - 27\,Hy^2 - 64\,(2917\,x^3 + 2052\,x^2 - 2493\,x - 514), \\
T_{43} &= 19683\,(13\,x^2 - 9)\,y^2 u - 864\,(1418\,x^3 + 129\,x^2 - 1692\,x - 59)\,u \\
&\quad - 8748\,(18\,x - 1)\,x^2 y^2 - 32\,(18952\,x^3 + 12663\,x^2 - 4734\,x - 943); \\
F &= (81\,y^2 + 162\,x^3 - 36\,x^2 - 154\,x - 72)\,u + 72\,x^3 - 4\,x^2, \\
G &= 27\,(18\,x - 1)\,y^2 + 243\,x^4 + 756\,x^3 - 270\,x^2 + 124\,x + 279, \\
H &= 1458\,x^3 - 729\,x^2 + 4158\,x + 1685,
\end{aligned}
$$

而 $\mathbb{U}_1 = \{x, T_{31}, T_{41}\}$.

对同样的变元序, $\mathbb{P}$ 的三角序列很容易由 TriSer 或 TriSerS 求得. 用 TriSer 可得五个良好三角系统, 其中的三角列与例 4.2.2 中列出的 $\mathbb{T}_i$ 完全一样; 用 TriSerS 可得四个良好三角系统, 其中两个三角列与上面的 $\mathbb{T}_1, \mathbb{T}_3$ 相同, 而另外两个与上面的 $\mathbb{T}_5, \mathbb{T}_6$ 稍有不同.

3.2 正则系统的性质

对任意三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$, 我们称 $\mathbb{T}$ 中多项式的导元为 $\mathbb{T}$ 的 *依量*, 而称这些导元之外的所有变元 x_i 为 $\mathbb{T}$ 的 *参量*.

定义 3.2.1 设 $\mathfrak{T} = [\mathbb{T}, \mathbb{U}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任意三角系统. 称 $\mathfrak{T}$ 的零点 $(\xi_1, \cdots, \xi_n)$ 为 *正则的*, 如果对任意 $1 \le i \le n$ 或者 $\xi_i = x_i$, 或者 x_i 是 $\mathbb{T}$ 的

依量.

若 $\mathfrak{T}$ 是正则的，那么 $\mathfrak{T}$ 的任意正则零点也称为 $\mathbb{T}$ 的 *正则零点*.

和通常一样，我们将 $\xi_1,\cdots,\xi_i$ 或 $(\xi_1,\cdots,\xi_i)$ 写为 $\boldsymbol{\xi}_i$，这里 $\boldsymbol{\xi}=\boldsymbol{\xi}_n$. $\mathrm{RegZero}(\mathfrak{T})$ 和 $\mathrm{RegZero}(\mathbb{T})$ 分别表示 $\mathfrak{T}$ 和 $\mathbb{T}$ 所有正则零点构成的集合. 显然 $\mathrm{RegZero}(\mathfrak{T})\subset\mathrm{Zero}(\mathfrak{T})$.

命题 3.2.1　正则列的正则零点之定义是适当的. 换言之，若 $[\mathbb{T},\mathbb{U}_1]$ 和 $[\mathbb{T},\mathbb{U}_2]$ 均为正则系统，则

$$\mathrm{RegZero}(\mathbb{T}/\mathbb{U}_1)=\mathrm{RegZero}(\mathbb{T}/\mathbb{U}_2).$$

证　设 $\boldsymbol{\xi}\in\mathrm{RegZero}(\mathbb{T}/\mathbb{U}_1)$. 首先考虑任意 $U\in\mathbb{U}_2$，其类 p 最小. 根据定义 x_p 是 $\mathbb{T}$ 的参量，因而 $\xi_p=x_p$ 是未定元. 于是 $U(\boldsymbol{\xi}_p)=0$ 蕴涵着 $\mathrm{ini}(U)(\boldsymbol{\xi}_{p-1})=0$. 由于 $[\mathbb{T},\mathbb{U}_2]$ 是正则系统，依据定义有 $\mathrm{ini}(U)(\boldsymbol{\xi}_{p-1})\neq0$. 由此可知 $U(\boldsymbol{\xi}_p)\neq0$.

现假定 $\mathbb{U}_2^{\langle i\rangle}\neq\emptyset$, 且对所有 $U\in\mathbb{U}_2^{(i-1)}$ 都有 $U(\boldsymbol{\xi}_{i-1})\neq0$, 那么

$$\boldsymbol{\xi}_{i-1}\in\mathrm{Zero}(\mathbb{T}^{(i-1)}/\mathbb{U}_2^{(i-1)}).$$

考虑任意 $U\in\mathbb{U}_2^{\langle i\rangle}$. 根据定义，$x_i$ 是 $\mathbb{T}$ 的参量; 因此 $\xi_i=x_i$. 由于 $[\mathbb{T},\mathbb{U}_2]$ 是正则的, 故 $\mathrm{ini}(U)(\boldsymbol{\xi}_{i-1})\neq0$. 鉴于同样理由 (如上), 我们有 $U(\boldsymbol{\xi}_i)\neq0$. 所以, 依据归纳原理, 对所有 $U\in\mathbb{U}_2$ 都有 $U(\boldsymbol{\xi})\neq0$. 这就证明了 $\boldsymbol{\xi}\in\mathrm{RegZero}(\mathbb{T}/\mathbb{U}_2)$; 因而 $\mathrm{RegZero}(\mathbb{T}/\mathbb{U}_1)\subset\mathrm{RegZero}(\mathbb{T}/\mathbb{U}_2)$. 用同样论点可以证明包含关系的另一方向. □

推论 3.2.2　对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意正则系统 $[\mathbb{T},\mathbb{U}]$ 以及 $\mathbb{T}$ 的正则零点 $\boldsymbol{\xi}$, $U(\boldsymbol{\xi})\neq0$ 对所有 $U\in\mathbb{U}$ 成立.

定义 3.2.2　$\mathcal{K}[\boldsymbol{x}]$ 中的三角系统 $\mathfrak{T}$ 称为在 $\tilde{\mathcal{K}}$ $(\supset\mathcal{K})$ 上是 *完美的*, 如果 $\tilde{\mathcal{K}}\text{-}\mathrm{Zero}(\mathfrak{T})\neq\emptyset$.

三角列 $\mathbb{T}\subset\mathcal{K}[\boldsymbol{x}]$ 称为在 $\tilde{\mathcal{K}}$ 上是 *完美的*, 如果 $[\mathbb{T},\mathrm{ini}(\mathbb{T})]$ 在 $\tilde{\mathcal{K}}$ 上是完美的.

$\mathcal{K}[\boldsymbol{x}]$ 中的三角列或系统称为是 *完美的* (不指定任何具体数域), 如果它在 $\mathcal{K}$ 的某个适当扩域上是完美的.

今将三角列 $\mathbb{T}$ 写成 (2.1.1) 的形式，并将导元 $x_{p_1},\cdots,x_{p_r}$ 重新命名为 $y_1,\cdots,y_r$ (它们是 $\mathbb{T}$ 的所有依量). 又用 $u_1,\cdots,u_d$，或缩写为 $\boldsymbol{u}$，来表示 $\{x_1,\cdots,x_n\}\setminus\{x_{p_1},\cdots,x_{p_r}\}$ 中的所有 x_i (即 $\mathbb{T}$ 的参量). 很明显 $d+r=n$. 因而 $\mathbb{T}$ 可以写成

$$\mathbb{T}=[T_1(\boldsymbol{u},y_1),\cdots,T_r(\boldsymbol{u},y_1,\cdots,y_r)]. \tag{3.2.1}$$

这时 $\mathfrak{T}$ 的任意正则零点具有下面的形式：

$$\boldsymbol{\xi}=(\boldsymbol{u},\eta_1,\cdots,\eta_r)\in \mathrm{Zero}(\mathfrak{T}), \tag{3.2.2}$$

这里对每个 i 有 $\eta_i\in\tilde{\mathcal{K}}\supset\mathcal{K}(\boldsymbol{u})$.

引理 3.2.3 $\mathcal{K}[\boldsymbol{x}]$ 中每个完美三角系统都有正则零点.

证 设 $\mathfrak{T}=[\mathbb{T},\mathbb{U}]$ 为一完美三角系统. 现将 $\mathbb{T}$ 写成 (3.2.1) 的形式，而

$$I_i(\boldsymbol{u},y_1,\cdots,y_{i-1})=\mathrm{ini}(T_i),\ 1\le i\le r,\quad V=\prod_{U\in\mathbb{U}}U.$$

由于在 $\mathcal{K}(\boldsymbol{u})$ 中 $I_1(\boldsymbol{u})\neq 0$，多项式 $T_1(\boldsymbol{u},y_1)$ 在 $\mathcal{K}(\boldsymbol{u})$ 的某一适当选取的代数扩域 $\tilde{\mathcal{K}}$ 中关于 y_1 必有零点. 又因为 $\mathfrak{T}$ 是完美的，所以 V 不可能在所有这些零点处都为零. 否则，T_1 的任意零点在 $\boldsymbol{u}$ 取特定的值之后也是 V 的零点；因而 $\mathfrak{T}$ 不是完美的. 由此可知，零点集

$$\mathcal{Z}_1=\{(\boldsymbol{u},\bar{y}_1):\ \bar{y}_1\in\tilde{\mathcal{K}},\ T_1(\boldsymbol{u},\bar{y}_1)=0,\ V(\boldsymbol{u},\bar{y}_1,y_2,\cdots,y_r)\neq 0\}$$

非空.

对任意 $(\boldsymbol{u},\bar{y}_1)\in\mathcal{Z}_1$，由三角系统的定义可知 $I_2(\boldsymbol{u},\bar{y}_1)\neq 0$；因此多项式 $T_2(\boldsymbol{u},\bar{y}_1,y_2)$ 在某一代数扩域 $\tilde{\mathcal{K}}$ 中关于 y_2 有零点. 依据同样理由，V 在 $(\boldsymbol{u},\bar{y}_1,\bar{y}_2)$ 处为零只可能对某些而不是对所有 $(\boldsymbol{u},\bar{y}_1)\in\mathcal{Z}_1$ 和 $\bar{y}_2\in\mathrm{Zero}(T_2(\boldsymbol{u},\bar{y}_1,y_2))$ 成立. 换言之，

$$\mathcal{Z}_2=\left\{(\boldsymbol{u},\bar{y}_1,\bar{y}_2):\ \begin{array}{l}(\boldsymbol{u},\bar{y}_1)\in\mathcal{Z}_1,\ \bar{y}_2\in\tilde{\mathcal{K}},T_2(\boldsymbol{u},\bar{y}_1,\bar{y}_2)=0,\\ V(\boldsymbol{u},\bar{y}_1,\bar{y}_2,y_3,\cdots,y_r)\neq 0\end{array}\right\}\neq\emptyset.$$

上面的推理可以对 T_3,T_4 等继续进行. 按照这种方式，我们最终将构造出 $\mathfrak{T}$ 的一个正则零点因而使引理获证. □

关于任意三角列 $\mathbb{T}$ 的 浸润sat($\mathbb{T}$), 参见定义 6.2.2. Zero(sat($\mathbb{T}$)) 表示所有以 $[\mathbb{T},\mathrm{ini}(\mathbb{T})]$ 的正则零点为一般点的不可约代数簇之并.

在正则零点 $\boldsymbol{\xi}$ 写成 (3.2.2) 的形式时, $\boldsymbol{\xi}_i$ 则代表 $\boldsymbol{u},\eta_1,\cdots,\eta_i$ 或 $(\boldsymbol{u},\eta_1,\cdots,\eta_i)$, 这里 $\boldsymbol{\xi}=\boldsymbol{\xi}_r$ 同前.

命题 3.2.4 设 $\mathbb{T}$, 如 (3.2.1) 所示, 为正则列, 那么对任意 $1\le i\le r-1$ 以及 $\boldsymbol{\xi}_i\in\mathrm{RegZero}(\mathbb{T}^{\{i\}})$ 都有

$$\mathrm{ini}(T_{i+1})(\boldsymbol{\xi}_i)\neq 0. \tag{3.2.3}$$

证 由于 $\mathbb{T}$ 是正则的, 所以存在 $\mathbb{U}$, 使得 $[\mathbb{T},\mathbb{U}]$ 为正则系统. 特别有 $\mathbb{U}\subset\mathcal{K}[\boldsymbol{u}]$. 对任意 $1\le i\le r-1$, 命 $\boldsymbol{\xi}_i\in\mathrm{RegZero}(\mathbb{T}^{\{i\}})$. 很明显, 对任意 $U\in\mathbb{U}$ 有 $U(\boldsymbol{\xi}_i)\neq 0$. 又因为 $[\mathbb{T},\mathbb{U}]$ 是三角系统, 依据定义 (3.2.3) 式成立. □

定义 3.2.3 设 P 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任一多项式, 而 $\mathbb{T}=[T_1,\cdots,T_r]$ 为三角列. 称多项式

$$\mathrm{res}(P,\mathbb{T})\triangleq\mathrm{res}(\cdots\mathrm{res}(P,T_r,\mathrm{lv}(T_r)),\cdots,T_1,\mathrm{lv}(T_1))$$

为 P 对 $\mathbb{T}$ 的 结式.

很明显, 对任意 i, $R=\mathrm{res}(P,\mathbb{T})$ 都不含有 $\mathrm{lv}(T_i)$. 若将变元 $\boldsymbol{x}$ 更名为 $\boldsymbol{u}$ 和 $\boldsymbol{y}$, 其中 $y_i=\mathrm{lv}(T_i)$, 那么 $R\in\mathcal{K}[\boldsymbol{u}]$.

引理 3.2.5 设 $\mathbb{T}=[T_1,\cdots,T_r]$ 为 $\mathcal{K}[\boldsymbol{z}]$ 中的三角列, P 为一多项式, 而 $R=\mathrm{res}(P,\mathbb{T})$, 那么在 $\mathcal{K}[\boldsymbol{z}]$ 中可求得多项式 Q 和 $Q_1,\cdots,Q_r$, 使得

$$QP=Q_1T_1+\cdots+Q_rT_r+R. \tag{3.2.4}$$

证 这是引理 1.3.1 的直接推论. □

命题 3.2.6 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意正则列 $\mathbb{T}$ 与多项式 P,

$$\mathrm{res}(P,\mathbb{T})\neq 0 \iff P(\boldsymbol{\xi})\neq 0 \text{ 对任意 } \boldsymbol{\xi}\in\mathrm{RegZero}(\mathbb{T}) \text{ 成立}.$$

证 ($\Longrightarrow$) 将变元 $\boldsymbol{x}$ 重新命名使 $\mathbb{T}$ 写成 (3.2.1) 的形式. 如果存在 $\boldsymbol{\xi}\in\mathrm{RegZero}(\mathbb{T})$ 使得 $P(\boldsymbol{\xi})=0$, 那么将 $\boldsymbol{\xi}$ 代入 (3.2.4) 式即得 $R=\mathrm{res}(P,\mathbb{T})=0$. 这与 $R\neq 0$ 的假设矛盾.

($\Longleftarrow$) 令

$$R_1 = R_1(\boldsymbol{z}_{r-1}) = \mathrm{res}(P, T_r, y_r), \quad \text{而} \quad \boldsymbol{\xi}_{r-1} \in \mathrm{RegZero}(\mathbb{T}^{\{r-1\}}).$$

由于 $\mathbb{T}$ 是正则的，依命题 3.2.4 我们有 $\mathrm{ini}(T_r)(\boldsymbol{\xi}_{r-1}) \neq 0$. 若 $R_1(\boldsymbol{\xi}_{r-1}) = 0$, 则 $P(\boldsymbol{\xi}_{r-1}, y_r)$ 和 $T_r(\boldsymbol{\xi}_{r-1}, y_r)$ 关于 y_r 有公共零点 η_r. 这是不可能的：原因是

$$\boldsymbol{\xi} \in \mathrm{RegZero}(\mathbb{T}), \quad P(\boldsymbol{\xi}) = 0$$

与 $P(\boldsymbol{\xi}) \neq 0$ ($\forall \boldsymbol{\xi} \in \mathrm{RegZero}(\mathbb{T})$) 的假设相矛盾. 所以对任意

$$\boldsymbol{\xi}_{r-1} \in \mathrm{RegZero}(\mathbb{T}^{\{r-1\}})$$

都有 $R_1(\boldsymbol{\xi}_{r-1}) \neq 0$.

接下来考虑 $R_2 = \mathrm{res}(R_1, T_{r-1}, y_{r-1})$, 且使用同样的论证. 我们将看出 $R_2(\boldsymbol{\xi}_{r-2}) \neq 0$ 对任意 $\boldsymbol{\xi}_{r-2} \in \mathrm{RegZero}(\mathbb{T}^{\{r-2\}})$ 都成立. 如此下去，最终将有 $R(\boldsymbol{u}) = R_r(\boldsymbol{u}) \neq 0$. 证毕. □

由命题 3.2.4 和 3.2.6 可得下面的结果.

推论 3.2.7 对任意正则列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 以及任意 $I \in \mathrm{ini}(\mathbb{T})$ 都有

$$\mathrm{res}(I, \mathbb{T}) \neq 0.$$

上述推论中的结论也是任意三角列为正则列的充分条件. 现将这一事实叙述如下.

引理 3.2.8 设 $\mathbb{T} = [T_1, \cdots, T_r]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的三角列，且假定

$$\mathrm{res}(\mathrm{ini}(T_i), \mathbb{T}^{\{i-1\}}) \neq 0, \quad 2 \leq i \leq r,$$

那么 $\mathbb{T}$ 是正则的.

证 命

$$R_1 = \mathrm{ini}(T_1) \prod_{i=2}^{r} \mathrm{res}(\mathrm{ini}(T_i), \mathbb{T}^{\{i-1\}}),$$

那么 R_1 不为 0 且不含有 $\mathrm{lv}(T_i)$. 又命 $R_i = \mathrm{ini}(R_{i-1})$, $i = 2, \cdots, t$, 使得 R_t 为常数. 按照定义，容易验证 $[\mathbb{T}, \{R_1, \cdots, R_t\}]$ 为正则系统. 由此引理立即获证. □

设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任意三角列. 总结上述结果，我们有下列等价条件:

(a) $\mathbb{T}$ 是正则的;

(b) 对任意 $I \in \mathrm{ini}(\mathbb{T})$ 有 $\mathrm{res}(I, \mathbb{T}) \neq 0$;

(c) 或者 $|\mathbb{T}| = 1$, 或者 $\mathbb{T}^{\langle n-1\rangle}$ 是正则的, 且

$$I(\boldsymbol{\xi}_{n-1}) \neq 0 \quad \text{对}\ I \in \mathrm{ini}(\mathbb{T}^{\langle n\rangle})\ \text{及所有}\ \boldsymbol{\xi}_{n-1} \in \mathrm{RegZero}(\mathbb{T}^{\langle n-1\rangle})\ \text{成立}.$$

因而, 条件 (b) 和 (c) 中任意一个都可以用作正则列的定义. 事实上, 它们已分别在文献 [105] 和 [35] 中用来定义等价的概念 正常升链 和 正则链. 条件 (b) 可作为判别任给三角列是否为正则列的有效准则. 命题 3.2.6, 推论 3.2.7 和引理 3.2.8 中的结果也已在文献 [105] 中给出.

命题 3.2.9 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的正则列, 而 P 为任一多项式, 那么

(a) $P(\boldsymbol{\xi}) \neq 0$ 对任意 $\boldsymbol{\xi} \in \mathrm{RegZero}(\mathbb{T})$ 成立

$$\iff \mathrm{RegZero}(\mathbb{T}) \cap \mathrm{Zero}(P) = \emptyset;$$

(b) $\mathrm{Zero}(\mathrm{sat}(\mathbb{T})) \subset \mathrm{Zero}(P) \iff \mathrm{RegZero}(\mathbb{T}) \subset \mathrm{Zero}(P)$.

该命题中的 (a) 是显然的, 而 (b) 可从浸润的定义得出.

与定理 3.4.4 和推论 4.5.9 相对应, 我们有下面的定理. 该定理的证明以及之后的定理 3.2.12 需要用到 6.2 节中给出的结果 (见定义 6.2.3 和定理 6.2.4).

定理 3.2.10 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意正则系统 $[\mathbb{T}, \mathbb{U}]$ 和多项式 P, $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(P)$ 当且仅当存在整数 $d > 0$, 使得 $\mathrm{prem}(P^d, \mathbb{T}) = 0$.

证 充分性从伪余公式和正则系统的定义立即可得.

为了证明必要性, 我们假定 $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(P)$, 令

$$V = \prod_{U \in \mathbb{U}} \mathrm{res}(U, \mathbb{T}),$$

并将 $\mathbb{T}$ 写成 (3.2.1) 的形式, 其中对 $1 \leq i \leq r$ 有 $\mathrm{ini}(T_i) = I_i$ 及 $\mathrm{ldeg}(T_i) = d_i$, 那么 (根据推论 3.2.2 与命题 3.2.6) 有 $V \in \mathcal{K}[\boldsymbol{u}]$, $V \neq 0$, 且 (由引理 3.2.5)

$$\mathrm{Zero}(\mathbb{T}/V) \subset \mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(P).$$

由此可知 $\mathrm{Zero}(\mathbb{T}/VP) = \emptyset$. 我们对 r 用归纳法来论证下面的断言, 以此完成定理的证明:

(A) 对任意正则列 $\mathbb{T}$ 与非零多项式 $V \in \mathcal{K}[\boldsymbol{u}]$ 及 $P \in \mathcal{K}[\boldsymbol{u}, y_1, \cdots, y_r]$ 如上, 若 $\mathrm{Zero}(\mathbb{T}/VP) = \emptyset$, 则存在整数 $d > 0$, 使得 $\mathrm{prem}(P^d, \mathbb{T}) = 0$.

首先考虑情形 $r=1$, 且命 $R=\operatorname{prem}(P^{d_1},T_1)$. 我们用 $R_1,\cdots,R_l$ 表示 R 关于 y_1 的所有非零系数. 按照引理 4.1.1 和 4.1.2 (b), 对所有 j 有 $\operatorname{Zero}(\emptyset/VR_j)=\emptyset$. 这就意味着 $R_j\equiv 0$ 对 $1\le j\le l$ 成立; 由此 $R\equiv 0$, 因而断言获证.

今设 (A) 对 $|\mathbb{T}|<r$ 的任意正则列 $\mathbb{T}$ 成立; 我们将证明 (A) 对 $|\mathbb{T}|=r>1$ 也成立. 设

$$\mathbb{T}^{\{r-1\}}=[T_1,\cdots,T_{r-1}],\quad J_{r-1}=I_1\cdots I_{r-1},\quad R=\operatorname{prem}(P^{d_r},T_r),$$

并用 $R_1,\cdots,R_l$ 表示 R 关于 y_r 的所有非零系数. 再使用引理 4.1.1 和 4.1.2 (b), 我们知道对所有 j 有 $\operatorname{Zero}(\mathbb{T}^{\{r-1\}}/VR_j)=\emptyset$. 依据归纳假设, 存在整数 $k_j>0$, 使得 $\operatorname{prem}(R_j^{k_j},\mathbb{T}^{\{r-1\}})=0$ 对所有 j 成立. 所以, 存在整数 $s_j\ge 0$, 使得

$$J_{r-1}^{s_j}R_j^{k_j}\in\operatorname{Ideal}(\mathbb{T}^{\{r-1\}}),\quad 1\le j\le l.$$

令

$$k=\max_{1\le j\le l}k_j,\quad s=\max_{1\le j\le l}s_j,$$

那么 $J_{r-1}^{s}R^{k}\in\operatorname{Ideal}(\mathbb{T})$. 另一方面, $R=\operatorname{prem}(P^{d_r},T_r)$ 意味着存在整数 $q_r\ge 0$, 使得 $I_r^{q_r}P^{d_r}-R\in\operatorname{Ideal}(\{T_r\})$. 所以

$$\begin{aligned}J_{r-1}^{s}I_r^{q_rk}P^{d_rk}&=J_{r-1}^{s}R^k+J_{r-1}^{s}(I_r^{q_r}P^{d_r}-R)[(I_r^{q_r}P^{d_r})^{k-1}+\cdots+R^{k-1}]\\&\in\operatorname{Ideal}(\mathbb{T}).\end{aligned}$$

令 $d=d_rk$ 及 $q=\max(s,q_rk)$, 则 $(I_1\cdots I_r)^qP^d\in\operatorname{Ideal}(\mathbb{T})$, 因此 $P^d\in\operatorname{sat}(\mathbb{T})$. 由定理 6.2.4, $P^d\in\operatorname{p-sat}(\mathbb{T})$, 因而 $\operatorname{prem}(P^d,\mathbb{T})=0$. 证毕. □

推论 3.2.11 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意正则列 $\mathbb{T}$ 与多项式 P, $\operatorname{Zero}(\mathbb{T}/\operatorname{ini}(\mathbb{T}))\subset\operatorname{Zero}(P)$ 当且仅当存在整数 $d>0$, 使得 $\operatorname{prem}(P^d,\mathbb{T})=0$.

证 充分性很显然, 所以我们只需证明必要性. 由于 $\mathbb{T}$ 是正则的, 所以存在多项式组 $\mathbb{U}\subset\mathcal{K}[\boldsymbol{x}]$, 使得 $[\mathbb{T},\mathbb{U}]$ 为正则系统, 且 $\operatorname{Zero}(\mathbb{T}/\mathbb{U})\subset\operatorname{Zero}(\mathbb{T}/\operatorname{ini}(\mathbb{T}))$. 若 $\operatorname{Zero}(\mathbb{T}/\operatorname{ini}(\mathbb{T}))\subset\operatorname{Zero}(P)$, 则 $\operatorname{Zero}(\mathbb{T}/\mathbb{U})\subset\operatorname{Zero}(P)$. 于是依定理 3.2.10, 存在整数 $d>0$, 使得 $\operatorname{prem}(P^d,\mathbb{T})=0$. □

读者可将下面的结果与定理 3.4.6 和 4.5.11 作一比较.

定理 3.2.12 设 $[\mathbb{P},\mathbb{Q}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统, 而 $[\mathbb{T}_1,\mathbb{U}_1],\cdots,[\mathbb{T}_e,\mathbb{U}_e]$ 为 $[\mathbb{P},\mathbb{Q}]$ 的正则序列, 那么:

(a) 存在整数 $d>0$, 使得 $\operatorname{prem}(P^d,\mathbb{T}_i)=0$ 对所有 $P\in\mathbb{P}$ 以及 $1\le i\le e$ 成立;

(b) 对任意整数 $m > 0$, $1 \le i \le e$ 和多项式 $Q \in \mathbb{Q}$ 都有

$$\text{prem}(Q^m, \mathbb{T}_i) \neq 0;$$

(c)

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\text{ini}(\mathbb{T}_i) \cup \mathbb{Q}). \tag{3.2.5}$$

证 (a) 由定义 3.1.1 可知

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\mathbb{U}_i),$$

因此 $\text{Zero}(\mathbb{T}_i/\mathbb{U}_i) \subset \text{Zero}(\mathbb{P}/\mathbb{Q}) \subset \text{Zero}(\mathbb{P})$ 对所有 i 成立. 依据定理 3.2.10, 存在整数 $d_{Pi} > 0$, 使得对任意 $P \in \mathbb{P}$ 与 $1 \le i \le e$ 都有 $\text{prem}(P^{d_{Pi}}, \mathbb{T}_i) = 0$, 所以 $P^{d_{Pi}} \in \text{sat}(\mathbb{T}_i)$. 置

$$d = \max_{\substack{P \in \mathbb{P} \\ 1 \le i \le e}} d_{Pi},$$

我们有 $P^d \in \text{sat}(\mathbb{T}_i)$, 因而根据定理 6.2.4, 对所有 $P \in \mathbb{P}$ 及 $1 \le i \le e$ 都有 $\text{prem}(P^d, \mathbb{T}_i) = 0$.

(b) 否则, 假定存在 $m > 0$, $1 \le i \le e$, 及 $Q \in \mathbb{Q}$, 使得 $\text{prem}(Q^m, \mathbb{T}_i) = 0$. 因此有

$$\text{Zero}(\mathbb{T}_i/\mathbb{U}_i) \subset \text{Zero}(\mathbb{T}_i/\text{ini}(\mathbb{T}_i)) \subset \text{Zero}(Q).$$

这与 $\text{Zero}(\mathbb{T}_i/\mathbb{U}_i) \subset \text{Zero}(\mathbb{P}/\mathbb{Q})$ 相矛盾.

(c) 由 (a) 及伪余公式可见, (3.2.5) 式的右边显然包含于该式的左边. 现在考虑任意 $\bar{\boldsymbol{x}} \in \text{Zero}(\mathbb{P}/\mathbb{Q})$, 则存在 i, 使得

$$\bar{\boldsymbol{x}} \in \text{Zero}(\mathbb{T}_i/\mathbb{U}_i) \subset \text{Zero}(\mathbb{T}_i/\text{ini}(\mathbb{T}_i) \cup \mathbb{Q}),$$

所以 $\bar{\boldsymbol{x}}$ 属于 (3.2.5) 式的右边. 定理获证. □

鉴于定理 3.2.12 (c), 在 $[\mathbb{T}_1, \mathbb{U}_1], \cdots, [\mathbb{T}_e, \mathbb{U}_e]$ 是 $\mathbb{P}$ 的正则序列时, 称 $\mathbb{T}_1, \cdots, \mathbb{T}_e$ 为 $\mathbb{P}$ 的 *正则序列* 是适当的.

设 $\mathfrak{T} = [\mathbb{T}, \mathbb{U}]$ 为正则系统, 并将 $\mathbb{T}$ 写成 (3.2.1) 的形式, 其中对每个 i 有 $\text{ini}(T_i) = I_i$. 又命

$$R = \prod_{U \in \mathbb{U}} \text{res}(U, \mathbb{T}) \in \mathcal{K}[\boldsymbol{u}].$$

那么，根据推论 3.2.2 和命题 3.2.6 有 $R \neq 0$, 并且

$$\mathrm{Zero}(\mathbb{T}/R) \subset \mathrm{Zero}(\mathfrak{T}).$$

很明显 $I_1(\boldsymbol{u}) \neq 0$, 因此 T_1 在 $\mathcal{K}(\boldsymbol{u})$ 中关于 y_1 有零点 η_1. 依命题 3.2.4, $I_2(\boldsymbol{u}, \eta_1) \neq 0$. 所以 $T_2(\boldsymbol{u}, \eta_1, y_2)$ 在 $\mathcal{K}(\boldsymbol{u})(\eta_1)$ 中关于 y_2 有零点 η_2. 因此，由命题 3.2.4 知 $I_3(\boldsymbol{u}, \eta_1, \eta_2) \neq 0$. 按这种方式进行下去，我们可以得到 $[\mathbb{T}, \{R\}]$ —— 因而 $\mathfrak{T}$ —— 的一个正则零点 $(\boldsymbol{u}, \eta_1, \cdots, \eta_r)$. 于是 $\mathfrak{T}$ 是完美的.

而且，对 $\boldsymbol{u}$ 的特定化 $\bar{\boldsymbol{u}}$, 我们也可以构造出 $\mathfrak{T}$ 的一个零点. 换言之，我们有下面的结论.

定理 3.2.13 $\mathcal{K}[\boldsymbol{x}]$ 中的所有正则系统在 $\mathcal{K}$ 的代数闭包 $\bar{\mathcal{K}}$ 上都是完美的.

证 设 $[\mathbb{T}, \mathbb{U}]$ 为正则系统，其中 $\mathbb{T} = [T_1, \cdots, T_r]$, 且

$$\mathrm{cls}(T_i) = p_i,\ \mathrm{ini}(T_i) = I_i,\quad 1 \leq i \leq r.$$

显然存在 $\bar{\boldsymbol{x}}_{p_1-1} \in \mathrm{Zero}(\emptyset/\mathbb{U}^{(p_1-1)})$. 因 $[\mathbb{T}, \mathbb{U}]$ 为三角系统，故 $I_1(\bar{\boldsymbol{x}}_{p_1-1}) \neq 0$. 所以 $T_1(\bar{\boldsymbol{x}}_{p_1-1}, x_{p_1})$ 在 $\mathcal{K}$ 的某一代数扩域中关于 x_{p_1} 有零点 $\bar{x}_{p_1}$. 由于 $\mathbb{U}^{\langle p_1\rangle} \doteq \emptyset$ 且 $\mathrm{ini}(U)(\bar{\boldsymbol{x}}_{j-1}) \neq 0$ 对任意 $U \in \mathbb{U}^{\langle j\rangle}$, $\bar{\boldsymbol{x}}_{j-1} \in \mathrm{Zero}(T_1/\mathbb{U}^{(j-1)})$ 及 $j = p_1 + 1, \cdots, p_2 - 1$ 成立，我们可以在 $\bar{\mathcal{K}}$ 中选取 $\bar{x}_{p_1+1}, \cdots, \bar{x}_{p_2-1}$, 使得

$$\bar{\boldsymbol{x}}_{p_2-1} \in \mathrm{Zero}(T_1/\mathbb{U}^{(p_2-1)}).$$

因此 $[\mathbb{T}, \mathbb{U}]$ 为三角系统意味着 $I_2(\bar{\boldsymbol{x}}_{p_2-1}) \neq 0$. 所以 $T_2(\bar{\boldsymbol{x}}_{p_2-1}, x_{p_2})$ 在 $\mathcal{K}$ 的某一代数扩域中关于 x_{p_2} 有零点 $\bar{x}_{p_2}$. 继续这一方式，我们最终将构造出 $[\mathbb{T}, \mathbb{U}]$ 的一个零点 $\bar{\boldsymbol{x}}$, 因而在 $\bar{\mathcal{K}}$ 中 $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \neq \emptyset$. □

我们将这一定理的若干推论罗列如下.

推论 3.2.14 $\mathcal{K}[\boldsymbol{x}]$ 中每个正则系统都具有强投影性质.

证 设 $[\mathbb{T}, \mathbb{U}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的正则系统. 容易验证，对任意 $0 < i < n$ 和 $\bar{\boldsymbol{x}}_i \in \mathrm{Zero}(\mathbb{T}^{(i)}/\mathbb{U}^{(i)})$, $[\mathbb{T}^{[i]\langle\bar{x},i\rangle}, \mathbb{U}^{[i]\langle\bar{x},i\rangle}]$ 是 $\mathcal{K}(\bar{\boldsymbol{x}}_i)[x_{i+1}, \cdots, x_n]$ 中的正则系统. 于是由定义 4.1.2 和定理 3.2.13 即知 $[\mathbb{T}, \mathbb{U}]$ 具有强投影性质. □

推论 3.2.15 每个正则列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 都是完美的.

证　由于 $\mathbb{T}$ 是正则的，所以存在多项式组 $\mathbb{U}$，使得 $[\mathbb{T},\mathbb{U}]$ 是正则的，因而 $\mathrm{Zero}(\mathbb{T}/\mathbb{U})\neq\emptyset$. 再由 $\mathrm{Zero}(\mathbb{T}/\mathbb{U})\subset\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T}))$ 和定理 3.2.13 即知 $\mathbb{T}$ 完美. □

推论 3.2.16　对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意多项式系统 $\mathfrak{P}$, $\mathrm{Zero}(\mathfrak{P})=\emptyset$ 当且仅当 $\mathfrak{P}$ 的每个正则序列都是空的.

推论 3.2.17　设 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统，而 P 为任意多项式. 又设 Ψ^* 为 $[\mathbb{P},\mathbb{Q}\cup\{P\}]$ 的任一正则序列，那么

$$\mathrm{Zero}(\mathfrak{P})\subset\mathrm{Zero}(P)\iff\Psi^*=\emptyset.$$

第六章中将给出任意三角列的若干结果，从那些结果可以得到正则系统的一些其他性质，譬如等维性.

3.3 分解为简单系统

我们在本节中引进简单系统的概念，该系统具有若干完美三角系统所不具备的良好特性. 粗略地说，简单系统是正则系统附加无平方因子的条件. 我们对算法 TriSerS 进行扩展使之可以计算这样的简单系统. 对任意多项式系统 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$，定义

$$\breve{\mathfrak{P}}=\mathbb{P}\cup\mathbb{Q}.$$

又回顾一下记号 $\boldsymbol{x}_i\triangleq(x_1,\cdots,x_i)$, $\bar{\boldsymbol{x}}_i\triangleq(\bar{x}_1,\cdots,\bar{x}_i)$，等.

对任意 $P\in\mathcal{K}[\boldsymbol{x}_k]$ 以及 $\mathcal{K}$ 的某一扩域 $\tilde{\mathcal{K}}$ 中的 $\bar{\boldsymbol{x}}_{k-1}$，称多项式 $P(\bar{\boldsymbol{x}}_{k-1},x_k)$ (关于 x_k) *无平方因子*，如果

$$\gcd\left(P(\bar{\boldsymbol{x}}_{k-1},x_k),\frac{\partial P}{\partial x_k}(\bar{\boldsymbol{x}}_{k-1},x_k)\right)\in\tilde{\mathcal{K}}.$$

例如，关于 x_2，多项式 $x_2^2-x_1$ 在 $x_1=1$ 时无平方因子，但在 $x_1=0$ 时并非无平方因子.

定义 3.3.1　称 $\mathfrak{S}=[\mathbb{T},\tilde{\mathbb{T}}]$ 为 *简单系统*，其中 $\mathbb{T}$ 和 $\tilde{\mathbb{T}}$ 或者是 $\mathcal{K}[\boldsymbol{x}]$ 中的三角列或者是空集，如果

(a) $\mathbb{T}\cap\tilde{\mathbb{T}}=\emptyset$，且 $\breve{\mathfrak{S}}$ 可被重排为三角列；

(b) 对每个类为 p 的多项式 $P\in\breve{\mathfrak{S}}$ 和任意 $\bar{\boldsymbol{x}}_{p-1}\in\mathrm{Zero}(\mathfrak{S}^{(p-1)})$，

$$\mathrm{ini}(P)(\bar{\boldsymbol{x}}_{p-1})\neq0,\quad\text{且}\quad P(\bar{\boldsymbol{x}}_{p-1},x_p)\ \text{无平方因子}.$$

三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 称为是 **简单的**, 或 **简单列**, 如果 $[\mathbb{T}, \emptyset]$ 是简单系统, 或者存在另一三角列 $\tilde{\mathbb{T}}$, 使得 $[\mathbb{T}, \tilde{\mathbb{T}}]$ 为简单系统.

在提及三角系统 $\mathfrak{T}$ 时, 我们有时候也说 $\mathfrak{T}$ 是 **简单的**. 很自然, 这是指 $\mathfrak{T}$ 为简单系统. 简单系统的概念源自托马斯的著作 ([68] 第六章). 他所称的简单系统在我们的定义下是约化的本原简单系统.

例 3.3.1 考虑 $\mathbb{P} = \{P_1, P_2, P_3\}$, 其中

$$\begin{aligned}
P_1 &= x_2^2 - x_1, \\
P_2 &= x_2x_3^3 - 2\,x_1x_3^2 + x_3^2 + x_1x_2x_3 - 2\,x_2x_3 + x_1, \\
P_3 &= x_2x_3x_4 + x_4 + x_1x_3 + x_2.
\end{aligned}$$

又设 $x_1 \prec \cdots \prec x_4$. 多项式 P_1, P_2, P_3 在 $\mathbb{Q}$ 上都是不可约的. 容易看出

- $\operatorname{ini}(P_1) = 1$, $I_2 = \operatorname{ini}(P_2) = x_2$, $I_3 = \operatorname{ini}(P_3) = x_2x_3 + 1$,
- $\mathbb{T} = [P_1, P_2, P_3]$ 是三角列,
- $\mathfrak{T} = [\mathbb{T}, \{I_2, I_3\}]$ 是良好的约化三角系统.

但 $\mathfrak{T}$ 不是简单系统. 首先 $\operatorname{cls}(I_3) = \operatorname{cls}(P_2)$, $\operatorname{cls}(I_2) = \operatorname{cls}(P_1)$ 违背了条件 (a). 其次, 可以验证 P_2, 在以 P_1 为 x_2 之添加多项式的扩域 $\mathbb{Q}(x_1, x_2)$ 上, 有因子分解

$$P_2 \doteq (x_2x_3 + 1)\,(x_3 - x_2)^2.$$

因此关于 x_3, P_2 不是对任意 $(x_1, x_2) \in \operatorname{Zero}(P_1/I_2)$ 都无平方因子.

例 3.3.2 多项式和三角系统如例 2.4.1 所示. $[\mathbb{T}_2, \emptyset]$ 不是简单系统; 原因是, 关于 y, 多项式 $y^2 - r^2 + 1$ 在 $r = \pm 1 \in \operatorname{Zero}(T)$ 时并非无平方因子, 这里

$$T = r^4 - 4\,r^2 + 3.$$

由于 $\operatorname{lv}(G) = x \in \mathbb{U}_1$, 所以 $\mathbb{T}_1 \cup \mathbb{U}_1$ 不能排成三角列; 因此 $[\mathbb{T}_1, \mathbb{U}_1]$ 也不是简单系统.

作为进一步说明, 考虑 $\mathfrak{T} = [\mathbb{T}_1, \{T\}]$, 它是三角系统. 这一点可验证如下: $\operatorname{ini}(P_2) = x = 0$, 且只在 $z = \pm 1$ 和 $r = \pm 1$ 或 $r^2 = 3$ 时有 $H = G = 0$. 这只有在 $T = 0$ 时才可能. 所以, 若 $H = G = 0$ 且 $T \neq 0$, 则 $x \neq 0$. 对 $\mathfrak{T}$, 条件 (a) 是满足的. 但 $\mathfrak{T}$ 也不是简单系统; 原因是, 关于 z, H —— 例如在 $27\,r^2 - 31 = 0$ 时 —— 不是无平方因子 (注意 $27\,r^2 - 31$ 与 T 互素).

定义 3.3.2 $\mathcal{K}[\boldsymbol{x}]$ 中的三角系统 $\mathfrak{T}$ 称为是 *本原的*, 如果每个 $P \in \mathfrak{T}$ 关于其导元都是本原的.

引理 3.3.1 设 $[\mathbb{T}, \tilde{\mathbb{T}}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的简单系统，而

$$\mathbb{T}^* = [\mathrm{pp}(T, \mathrm{lv}(T)) \colon T \in \mathbb{T}], \quad \tilde{\mathbb{T}}^* = [\mathrm{pp}(T, \mathrm{lv}(T)) \colon T \in \tilde{\mathbb{T}}],$$

那么 $[\mathbb{T}^*, \tilde{\mathbb{T}}^*]$ 是一本原简单系统，使得

$$\mathrm{Zero}(\mathbb{T}^*/\tilde{\mathbb{T}}^*) = \mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}}).$$

证 由于任意多项式的本原部分与该多项式本身具有相同的类，因而 $\mathbb{T}^*$, $\tilde{\mathbb{T}}^*$ 和 $\mathbb{T}^* \cup \tilde{\mathbb{T}}^*$ 都能被重排为三角列. 于是我们只需说明对任意类为 p 的多项式 $T \in \mathbb{T} \cup \tilde{\mathbb{T}}$ 以及

$$\bar{\boldsymbol{x}}_{p-1} \in \mathrm{Zero}(\mathbb{T}^{(p-1)}/\tilde{\mathbb{T}}^{(p-1)})$$

都有 $\mathrm{cont}(T, x_p)(\bar{\boldsymbol{x}}_{p-1}) \neq 0$, 因此 $\mathrm{cont}(T, x_p)$ 可从 T 中抹去. 这是明显的，因为 $\mathrm{cont}(T, x_p)$ 是 $\mathrm{ini}(T)$ 的因子，而根据定义又有 $\mathrm{ini}(T)(\bar{\boldsymbol{x}}_{p-1}) \neq 0$. □

鉴于这一引理，我们可以随意 —— 特别是在举例计算时 —— 将简单系统化为本原的.

引理 3.3.2 设 P_1 和 P_2 为 $\mathcal{K}[\boldsymbol{x}_k]$ 中满足 $\deg(P_1, x_k) \geq \deg(P_2, x_k) > 0$ 的多项式，$H_2, \cdots, H_r$ 为 P_1 和 P_2 关于 x_k 的子结式正则子链，而

$$I = \mathrm{lc}(P_2, x_k), \quad I_i = \mathrm{lc}(H_i, x_k), \quad 2 \leq i \leq r.$$

又设 $\mathbb{P}, \mathbb{Q} \subset \mathcal{K}[\boldsymbol{x}_{k-1}]$ 为多项式组，并假定对任意 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 有 $I(\bar{\boldsymbol{x}}_{k-1}) \neq 0$, 而 $P_2(\bar{\boldsymbol{x}}_{k-1}, x_k)$ 无平方因子，那么

$$\mathrm{Zero}(\mathbb{P} \cup \{P_2\}/\mathbb{Q} \cup \{P_1\}) = \bigcup_{i=2}^{r} \mathrm{Zero}(\mathbb{P} \cup \mathbb{P}_i/\mathbb{Q} \cup \{I_i\}), \tag{3.3.1}$$

其中 $\mathbb{P}_i = \{\mathrm{pquo}(P_2, H_i, x_k), I_{i+1}, \cdots, I_r\}$, $2 \leq i \leq r$.

证 参阅引理 3.1.1 的证明. 对任意 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$, 必定存在 i $(2 \leq i \leq r)$, 使得 (3.1.4) 和 (3.1.5) 成立. 由于 $P_2(\bar{\boldsymbol{x}}_{k-1}, x_k)$ 无平方因子，零点关系 (3.3.1) 显而易见. □

注意，在 (3.3.1) 式的右边 P_1 不再出现，而对每个 i 仅有一个类为 k 的多项式 $\mathrm{pquo}(P_2, H_i, x_k)$. 在这种意义下，多项式 P_1 通过分裂而被消去. 下述引理中分裂的目的在于将任一多项式变成无平方因子.

引理 3.3.3 设 P 为 $\mathcal{K}[\boldsymbol{x}_k]$ 中的多项式，而 $\deg(P, x_k) > 1$, $I = \mathrm{lc}(P, x_k)$. 又设 $H_2, \cdots, H_r$ 为 P 及其导数 $\partial P/\partial x_k$ 关于 x_k 的子结式正则子链，而

$$H_2^* = H_2, \quad H_i^* = \frac{H_i}{I}, \ 3 \le i \le r; \quad I_i = \mathrm{lc}(H_i^*, x_k), \ 2 \le i \le r,$$

那么

$$\mathrm{Zero}(P/I) = \bigcup_{i=2}^{r} \mathrm{Zero}(\{Q_i, I_{i+1}, \cdots, I_r\}/II_i), \tag{3.3.2}$$

$$\mathrm{Zero}(\emptyset/PI) = \bigcup_{i=2}^{r} \mathrm{Zero}(\{I_{i+1}, \cdots, I_r\}/Q_iII_i), \tag{3.3.3}$$

其中 $Q_i = \mathrm{pquo}(P, H_i^*, x_k)$, $2 \le i \le r$. 而且，对任意 $2 \le i \le r$ 与

$$\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\{I_{i+1}, \cdots, I_r\}/II_i),$$

$Q_i(\bar{\boldsymbol{x}}_{k-1}, x_k)$ 都无平方因子.

证 显然 $\mathrm{lc}(\partial P/\partial x_k, x_k) = \deg(P, x_k)\, I$. 从子结式的定义容易看出，对 $3 \le i \le r$, I 整除 H_i. 作为代数学中的基本事实，我们知道对任意 $2 \le i \le r$ 以及 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\{I_{i+1}, \cdots, I_r\}/II_i)$,

$$P(\bar{\boldsymbol{x}}_{k-1}, x_k)/\gcd\left(P(\bar{\boldsymbol{x}}_{k-1}, x_k), \frac{\partial P}{\partial x_k}(\bar{\boldsymbol{x}}_{k-1}, x_k)\right)$$

都无平方因子，而且关于 x_k 它与 $P(\bar{\boldsymbol{x}}_{k-1}, x_k)$ 具有相同的零点集. $Q_i(\bar{\boldsymbol{x}}_{k-1}, x_k)$ 无平方因子以及零点关系式 (3.3.2) 和 (3.3.3) 从这一事实与引理 2.4.2 (a) 立即可得. □

定义 3.3.3 有限多个 $\mathcal{K}[\boldsymbol{x}]$ 中的简单系统 $\mathfrak{S}_1, \cdots, \mathfrak{S}_e$ 构成的集合或序列称为 *简单序列*. 又称该序列为多项式系统 $\mathfrak{P}$ 的 *简单序列*, 如果零点分解

$$\mathrm{Zero}(\mathfrak{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathfrak{S}_i) \tag{3.3.4}$$

成立. 也称 $[\mathbb{P}, \emptyset]$ 的简单序列为多项式组 $\mathbb{P}$ 的 *简单序列*.

下面的算法是为计算任给多项式系统的简单序列而设计的. 它同样使用从上到下 (即由 x_n 至 x_1) 且带分裂的消元策略. 不难发现, 该算法是 TriSerS 和 RegSer 的扩展. (在列举循环 S2.2 中) 对每个 x_k 主要有下列四步:

S2.2.1 从 $\mathbb{T}^{\langle k\rangle} \neq \emptyset$ 产生类为 k 的单个多项式 P_2;

S2.2.2 将 P_2 变为关于 x_k 无平方因子;

S2.2.3 用 P_2 将 $\tilde{\mathbb{T}}^{\langle k\rangle} \neq \emptyset$ 中的多项式消去;

S2.2.4 从 $\tilde{\mathbb{T}}^{\langle k\rangle} \neq \emptyset$ 产生单个关于 x_k 无平方因子的多项式 P_1.

而整个算法中又有下述三种分裂:

(i) 在步骤 S2.2.1.1 和 S2.2.4.1 中按照所考虑的多项式之初式是否为零 (或者假定该初式不为零或者将所述多项式用其初式和尾式来替代);

(ii) 在步骤 S2.2.1.3 和 S2.2.3.2 中按照引理 2.4.2 (b) 和 3.3.2 进行基本消元;

(iii) 在步骤 S2.2.2.2 和 S2.2.4.3 中按照引理 3.3.3 实现无平方因子.

算法 SimSer: $\Psi \leftarrow \mathrm{SimSer}(\mathbb{P},\mathbb{Q})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P},\mathbb{Q}]$, 本算法计算 $[\mathbb{P},\mathbb{Q}]$ 的简单序列 Ψ.

S1. 命 $\Phi \leftarrow \{[\mathbb{P},\mathbb{Q},n]\}, \Psi \leftarrow \emptyset$.

S2. 重复下列步骤直至 $\Phi = \emptyset$:

S2.1. 设 $[\mathbb{T},\tilde{\mathbb{T}},\ell]$ 为 Φ 中的元素, 且命 $\Phi \leftarrow \Phi \setminus \{[\mathbb{T},\tilde{\mathbb{T}},\ell]\}$.

S2.2. 对 $k = \ell,\cdots,1$ 执行下列步骤:

S2.2.1. 重复下列步骤直至 $\mathbb{T}^{\langle k\rangle} = \emptyset$:

S2.2.1.1. 设 P_2 为 $\mathbb{T}^{\langle k\rangle}$ 中关于 x_k 次数最小的多项式, 且命

$$\Phi \leftarrow \Phi \cup \{[\mathbb{T} \setminus \{P_2\} \cup \{\mathrm{ini}(P_2), \mathrm{red}(P_2)\}, \tilde{\mathbb{T}}, k]\},$$
$$\tilde{\mathbb{T}} \leftarrow \tilde{\mathbb{T}} \cup \{\mathrm{ini}(P_2)\}.$$

若 $|\mathbb{T}^{\langle k\rangle}| = 1$, 则转至 S2.2.2; 否则, 从 $\mathbb{T}^{\langle k\rangle} \setminus \{P_2\}$ 中选取多项式 P_1.

S2.2.1.2. 计算 P_1 和 P_2 关于 x_k 的子结式正则子链 $H_2,\cdots,H_r$, 且对 $2 \leq i \leq r$ 命 $I_i \leftarrow \mathrm{lc}(H_i, x_k)$. 若 $\mathrm{cls}(H_r) < k$, 则命 $\bar{r} \leftarrow r-1$; 否则命 $\bar{r} \leftarrow r$.

S2.2.1.3. 命

$$\begin{aligned}&\Phi\leftarrow\Phi\cup\{[\mathbb{T}\setminus\{P_1,P_2\}\cup\{H_i,I_{i+1},\cdots,I_r\},\\&\qquad\qquad\tilde{\mathbb{T}}\cup\{I_i\},k]:\ 2\le i\le\bar{r}-1\},\\&\mathbb{T}\leftarrow\mathbb{T}\setminus\{P_1,P_2\}\cup\{H_r,H_{\bar{r}}\},\\&\tilde{\mathbb{T}}\leftarrow\tilde{\mathbb{T}}\cup\{I_{\bar{r}}\}.\end{aligned}$$

S2.2.2. 若 $\mathbb{T}^{\langle k\rangle}=\emptyset$, 则转至 S2.2.4. 若 $\deg(P_2,x_k)=1$, 则转至 S2.2.3; 否则:

S2.2.2.1. 计算 P_2 及其导数 $\partial P_2/\partial x_k$ 关于 x_k 的子结式正则子链 $H_2,\cdots,H_r$, 且命

$$\begin{aligned}&H_2^*\leftarrow H_2,\quad H_i^*\leftarrow H_i/\mathrm{ini}(P_2),\ i=3,\cdots,r,\\&I_i\leftarrow\mathrm{lc}(H_i^*,x_k),\quad i=2,\cdots,r.\end{aligned}$$

若 $\tilde{\mathbb{T}}^{\langle k\rangle}=\emptyset$, 则命 $\bar{k}\leftarrow k-1$; 否则命 $\bar{k}\leftarrow k$.

S2.2.2.2. 命

$$\begin{aligned}&\Phi\leftarrow\Phi\cup\{[\mathbb{T}\setminus\{P_2\}\cup\{\mathrm{pquo}(P_2,H_i^*,x_k),I_{i+1},\cdots,I_r\},\\&\qquad\qquad\tilde{\mathbb{T}}\cup\{I_i\},\bar{k}]:\ 2\le i\le r-1\},\\&\mathbb{T}\leftarrow\mathbb{T}\setminus\{P_2\}\cup\{\mathrm{pquo}(P_2,H_r^*,x_k)\},\\&\tilde{\mathbb{T}}\leftarrow\tilde{\mathbb{T}}\cup\{I_r\},\\&P_2\leftarrow\mathrm{pquo}(P_2,H_r^*,x_k).\end{aligned}$$

S2.2.3. 重复下列步骤直至 $\tilde{\mathbb{T}}^{\langle k\rangle}=\emptyset$ 或者 $\mathrm{cls}(P_2)\neq k$:

S2.2.3.1. 设 P_1 为 $\tilde{\mathbb{T}}^{\langle k\rangle}$ 中的多项式. 计算 P_1 和 P_2 —— 如果 $\deg(P_1,x_k)\ge\deg(P_2,x_k)$ —— 或者 P_2 和 P_1 —— 否则的话 —— 关于 x_k 的子结式正则子链 $H_2,\cdots,H_r$, 且对 $2\le i\le r$ 命 $I_i\leftarrow\mathrm{lc}(H_i,x_k)$.

S2.2.3.2. 命

$$\begin{aligned}&\Phi\leftarrow\Phi\cup\{[\mathbb{T}\setminus\{P_2\}\cup\{\mathrm{pquo}(P_2,H_i,x_k),I_{i+1},\cdots,I_r\},\\&\qquad\qquad\tilde{\mathbb{T}}\setminus\{P_1\}\cup\{I_i\},k]:\ 2\le i\le r-1\},\\&\mathbb{T}\leftarrow\mathbb{T}\setminus\{P_2\}\cup\{\mathrm{pquo}(P_2,H_r,x_k)\},\\&\tilde{\mathbb{T}}\leftarrow\tilde{\mathbb{T}}\setminus\{P_1\}\cup\{I_r\},\\&P_2\leftarrow\mathrm{pquo}(P_2,H_r,x_k).\end{aligned}$$

S2.2.4. 若 $\tilde{\mathbb{T}}^{\langle k\rangle}\neq\emptyset$, 则:

S2.2.4.1. 命

$$P_1 \leftarrow \prod_{P\in\tilde{\mathbb{T}}^{\langle k\rangle}} P,$$
$$\Phi \leftarrow \Phi \cup \{[\mathbb{T}\cup\{\mathrm{ini}(P_1)\}, \tilde{\mathbb{T}}\setminus\tilde{\mathbb{T}}^{\langle k\rangle}\cup\{\mathrm{red}(P_1)\}, k]\},$$
$$\tilde{\mathbb{T}} \leftarrow \tilde{\mathbb{T}}\cup\{\mathrm{ini}(P_1)\}.$$

若 $\deg(P_1, x_k) = 1$, 则转至 S2.2.5.

S2.2.4.2. 计算 P_1 及其导数 $\partial P_1/\partial x_k$ 关于 x_k 的子结式正则子链 $H_2, \cdots, H_r$, 且命

$$H_2^* \leftarrow H_2,\quad H_i^* \leftarrow H_i/\mathrm{ini}(P_1),\ i = 3, \cdots, r,$$
$$I_i \leftarrow \mathrm{lc}(H_i^*, x_k),\quad i = 2, \cdots, r.$$

S2.2.4.3. 命

$$\Phi \leftarrow \Phi \cup \{[\mathbb{T}\cup\{I_{i+1}, \cdots, I_r\}, \tilde{\mathbb{T}}\setminus\tilde{\mathbb{T}}^{\langle k\rangle}\cup \{\mathrm{pquo}(P_1, H_i^*, x_k), I_i\}, k-1]:\ 2\le i\le r-1\},$$
$$\tilde{\mathbb{T}} \leftarrow \tilde{\mathbb{T}}\setminus\tilde{\mathbb{T}}^{\langle k\rangle}\cup\{\mathrm{pquo}(P_1, H_r^*, x_k), I_r\}.$$

S2.2.5. 命 $\mathbb{T}\leftarrow\mathbb{T}\setminus\{0\}, \tilde{\mathbb{T}}\leftarrow\tilde{\mathbb{T}}\setminus(\mathcal{K}\setminus\{0\})$. 如果 $\mathbb{T}\cap\mathcal{K}\neq\emptyset$ 或 $0\in\tilde{\mathbb{T}}$, 则转至 S2.

S2.3. 命 $\Psi\leftarrow\Psi\cup\{[\mathbb{T},\tilde{\mathbb{T}}]\}$, 其中 $\mathbb{T}$ 和 $\tilde{\mathbb{T}}$ 在非空时排为三角列.

证 参阅 RegSer 的证明. 我们略去部分类似的论证.

正确性. 在 SimSer 的每种分裂情形, 也都是一个分裂的系统被用来更新当前系统 $[\mathbb{T},\tilde{\mathbb{T}}]$; 该系统对应于 (2.4.1) 和 (3.3.1)–(3.3.3) 中 $i = r$ 的情形, 但在 $\deg(H_r, x_k) = 0$ 时, 它对应于 (2.4.1) 式中情况 $i = r-1$ 的系统. 其他分裂的系统则被添入 Φ. 依据 (2.4.1), (3.3.1)–(3.3.3) 以及关于第一类分裂的明显零点关系, 形如 (3.1.6) 的零点分解总是成立. 于是我们最终将获得分解 (3.3.4), 其中 $\mathfrak{P} = [\mathbb{P},\mathbb{Q}]$. 根据定义, 所计算出的 Ψ 中的有序多项式组的对都是简单系统.

终止性. 步骤 S2.2.1 和 S2.2.3 与 RegSer 中的 R2.2.2 和 R2.2.3 相同, 它们显然终止. 在分裂的每种情形, 分裂了的多项式系统都是从当前系统通过两种方式获得的: 或者用一个关于其公共导元 x_k 有较低次数的多项式去替换一个或两个多项式 (正如在大多数情形), 或者用单个多项式去替换两个或多个具有相同类 k 的多项式 (如 S2.2.1.3 中在 $\bar{r} = 2$ 时和 S2.2.4.3 中在 $|\tilde{\mathbb{T}}^{\langle k\rangle}| > 1$ 时); 有时候类 $< k$ 的多项式则被添加进去. 所以, 循环 S2 也只能重复有限多次. □

注 3.3.1 如果 P_2 是先前 S2.2.2.2 中生成的 $\mathrm{pquo}(P_2, H_i^*, x_k)$ 或者 S2.2.3.2 中生成的 $\mathrm{pquo}(P_2, H_i, x_k)$ 之一，那么 SimSer 中的步骤 S2.2.2.1 和 S2.2.2.2 可以跳过去. 原因是此时已知 P_2 关于 x_k (有条件地) 无平方因子.

注 2.4.1 中提到的策略也应该在 TriSerP 和 SimSer 中实施以避免不必要的计算. 作进一步的约化有时候也能简化简单系统并使其变得更加规范. 譬如，我们可以要求简单系统都化为本原和约化的. 这一问题将在 5.1 节中讨论，尽管其解答对方法的理论发展和实际应用并没有多大贡献.

计算简单系统的动机之一源自托马斯的工作[68]. SimSer 与托马斯的方法具有相似的功能，而且它们的某些步骤也很相似. 但我们的算法在结构和基本运算上都与托马斯的很不一样.

例 3.3.3 设 $\mathbb{P}, P_i, \mathfrak{T}$ 与例 3.3.1 中相同，而

$$\mathbb{T}' = [P_1, x_2x_3 + 1], \quad \mathbb{T}'' = [x_1, \cdots, x_4],$$

那么，使用 SimSer 可将 $\mathbb{P}$ 分解为三个约化的简单系统

$$[[P_1, x_3 - x_2, x_4 + x_2], [x_1\,(x_1 + 1)]], \quad [\mathbb{T}', [x_1]], \quad [\mathbb{T}'', \emptyset]. \tag{3.3.5}$$

其过程大致如下. 置

$$[\mathbb{T}, \tilde{\mathbb{T}}] \leftarrow [\{P_1, P_2, P_3\}, \{x_2, I_3\}] = \mathfrak{T}.$$

P_3 关于 x_4 是线性的，因而无平方因子. 为使 P_2 关于 x_3 无平方因子，计算 P_2 和 $\partial P_2/\partial x_3$ 关于 x_3 的子结式正则子链，该链为

$$\frac{\partial P_2}{\partial x_3}, \quad 2\,x_2H_1, \quad 4\,x_2H_2,$$

其中 H_1 是 x_3 的线性多项式，而 H_2 是一个类为 2 的多项式. 注意 $x_2 \in \tilde{\mathbb{T}}$，因此有两种情形： (i) $H_2 \neq 0$ 且 P_2 关于 x_3 无平方因子； (ii) $H_2 = 0, I = \mathrm{ini}(H_1) \neq 0$，且 P_2 被 $\mathrm{pquo}(P_2, H_1, x_3)$ 所替代，而后者关于 x_3 无平方因子. 为简化计算，我们指出 H_2 以 P_1 为因子. 所以，遵循算法程序时第一种情形将被排除，而对第二种情形则不必将 H_2 添入 $\mathbb{T}$. 故命

$$[\mathbb{T}, \tilde{\mathbb{T}}] \leftarrow [\{P_1, H_3, P_3\}, [x_2, I_3, I]],$$

其中 $H_3 = \mathrm{pquo}(P_2, H_1, x_3)$ 有 42 项，关于 x_3 的次数为 2，而 I 有 5 项，关于 x_2 的次数为 2.

以下我们希望用 H_3 将 I_3 从 $\tilde{\mathbb{T}}$ 中消去. 为此, 计算 H_3 和 I_3 关于 x_3 的子结式正则子链: I_3, H_4, 其中 H_4 是一个 20 项的多项式, 也以 P_1 为其因子, 故在 $x_1 \neq 0$ 时有 $\gcd(H_3, I_3, x_3) = I_3$. 所以置

$$[\mathbb{T}, \tilde{\mathbb{T}}] \leftarrow [\{P_1, H_5, P_3\}, \{x_1, x_2, I\}],$$

其中 $H_5 = \mathrm{pp}(\mathrm{pquo}(H_3, I_3, x_3), x_3)$ 有 11 项.

现在 P_1 关于 x_2 无平方因子, 且在 $x_1(x_1+1) \neq 0$ 时 $\gcd(P_1, x_2, x_2)$ 和 $\gcd(P_1, I, x_2)$ 都是常数. 因而获得简单系统 $[\{P_1, H_5, P_3\}, \{x_1\,(x_1+1)\}]$. 最后, 用

$$\begin{aligned}
&\mathrm{pp}(\mathrm{prem}(H_5, P_1, x_2), x_3) = x_3 - x_2,\\
&\mathrm{pp}(\mathrm{prem}(P_3, [P_1, x_3 - x_2]), x_3) = x_4 + x_2
\end{aligned}$$

分别替换 H_5 和 P_3, 我们得到 (3.3.5) 中的第一个约化的本原简单系统.

考虑从 $\mathbb{P}$ 分别用 P_2 和 P_3 的初式与尾式来替换它们本身所得的多项式组并遵照同样的程序, 我们将得到另外两个约化的简单系统.

顺便提及, 用 TriSerS 可以将 $\mathbb{P}$ 分解为三个良好的三角系统 $\mathfrak{T}, [\mathbb{T}', \{x_2\}]$, $[\mathbb{T}'', \emptyset]$.

例 3.3.4　设 $\mathbb{P}$ 与例 2.4.1 中相同, 并将那里的多项式 H, G, P_2 重新命名为 T_1, T_2, T_3:

$$\begin{aligned}
T_1 &= z^3 - z^2 + r^2 - 1,\\
T_2 &= x^4 + z^2x^2 - r^2x^2 + z^4 - 2\,z^2 + 1,\\
T_3 &= xy + z^2 - 1.
\end{aligned}$$

此外, 又命

$$T = r^8 - 6\,r^6 + 71\,r^4 - 62\,r^2 - 67.$$

用 SimSer 不难求得 $\mathbb{P}$ 的简单序列, 它由 9 个简单系统 $[\mathbb{T}_1, \tilde{\mathbb{T}}_1], \cdots, [\mathbb{T}_9, \tilde{\mathbb{T}}_9]$ 构成, 其中

$$\begin{aligned}
\mathbb{T}_1 &= [T_1, T_2, T_3],\\
\mathbb{T}_2 &= [r^2 - 1, z - 1, x, y],\\
\mathbb{T}_3 &= [r^2 - 1, z, x^4 - x^2 + 1, xy - 1],\\
\mathbb{T}_4 &= [r^2 - 3, z + 1, x^2 - 2, y],\\
\mathbb{T}_5 &= [r^2 - 3, z + 1, x, y^2 - 2],\\
\mathbb{T}_6 &= [r^2 - 3, z^2 - 2\,z + 2, T_2, T_3],\\
\mathbb{T}_7 &= [27\,r^2 - 31, 9\,z^2 - 3\,z - 2, 27\,x^4 + (9\,z - 25)\,x^2 - 13\,z + 17,\\
&\qquad 9\,xy + 3\,z - 7],
\end{aligned}$$

$$\begin{aligned}
\mathbb{T}_8 &= [T, (r^4 + 14\,r^2 + 15)\,z + 3\,r^4 + 13\,r^2 - 4,\\
&\qquad (z^2 + z + 1)\,x^2 + z^5 + z^4 - z^3 - 3\,z^2 + z + 1, T_3],\\
\mathbb{T}_9 &= [T, (34\,r^6 + 155\,r^4 + 482\,r^2 + 292)\,z^2 - (107\,r^6 + 165\,r^4\\
&\qquad + 807\,r^2 + 433)\,z + 205\,r^6 - 484\,r^4 + 779\,r^2 + 760, T_2, T_3];\\
\tilde{\mathbb{T}}_1 &= [(r^2 - 1)\,(r^2 - 3)\,(27\,r^2 - 31)\,T],\\
\tilde{\mathbb{T}}_2 &= \cdots = \tilde{\mathbb{T}}_9 = \emptyset.
\end{aligned}$$

在计算这一简单序列时，我们未使用多项式因子分解．如果将所出现的多项式分解为因子，输出结果会变得简单一些．

例 3.3.5 例 2.4.3 中给出的多项式组 $\mathbb{P}$ 的简单序列 —— 用 SimSer 对同样的变元序计算得出 —— 由 13 个简单系统 $[\mathbb{T}_1, \tilde{\mathbb{T}}_1], \cdots, [\mathbb{T}_{13}, \tilde{\mathbb{T}}_{13}]$ 构成，其中 $\mathbb{T}_1, \cdots, \mathbb{T}_7$ 与例 2.4.3 中的相同，而

$$\begin{aligned}
\mathbb{T}_8 &= [H_1, 36\,z^3 - 8\,c^2z^2 - 42\,cz + 81, H_4, P_3],\\
\mathbb{T}_9 &= [H_1, 2\,cz + 3, 2\,c^2y^2 - 3\,cy - 9, 3\,yx + 2\,c],\\
\mathbb{T}_{10} &= [2\,c^3 - 27, 2\,c^2z^2 + 3\,cz - 9, y - z, 2\,y^2x - xc + 1],\\
\mathbb{T}_{11} &= [H_2, H_3, H_4, P_3],\\
\mathbb{T}_{12} &= [H_2, H_3, zy - z^2 + c, x - z],\\
\mathbb{T}_{13} &= [H_2, 54\,(1938466\,c^3 + 138253)\,z^3 - 16\,(440494\,c^3 + 31419)\,c^2z^2\\
&\qquad - 9\,(4103430\,c^3 + 292663)\,cz - 3\,(7980362\,c^3 + 569169),\\
&\qquad (cz + 1)\,y + cz^2 - z, P_3];
\end{aligned}$$

$$\begin{aligned}
&\tilde{\mathbb{T}}_1 = \tilde{\mathbb{T}}_2 = [cH_2],\quad \tilde{\mathbb{T}}_3 = [H_1],\quad \tilde{\mathbb{T}}_4 = [cH_1H_2],\quad \tilde{\mathbb{T}}_5 = [2\,c^3 - 27],\\
&\tilde{\mathbb{T}}_6 = \cdots = \tilde{\mathbb{T}}_{13} = \emptyset;
\end{aligned}$$

$$\begin{aligned}
H_1 &= 4\,c^3 - 27,\\
H_2 &= 8\,c^6 - 378\,c^3 - 27,\\
H_3 &= 36\,(18\,c^3 + 1)\,z^3 + 8\,(10\,c^3 + 3)\,c^2z^2 - 2\,(250\,c^3 + 9)\,cz\\
&\qquad - 9\,(290\,c^3 + 21),\\
H_4 &= (z^3 - cz + 1)\,y + z^4 - 2\,cz^2 + c^2.
\end{aligned}$$

为获得该简单序列，计算时曾对某些中间多项式作了 $\mathbb{Q}$ 上的因子分解．

计算简单序列一般来说是很费时的．主要是因为将多项式化为无平方因子以及消去非方程多项式需要付出昂贵的代价．实际应用时，甚至宁可选用高效的多项式因子分解程序来计算不可约三角序列而代之．这将在第四章中予以说明．

3.4 简单系统的性质

引进简单系统的部分意义可以从本节中给出并证明的性质看出. 现用 $\bar{\mathcal{K}}$ 表示基域 $\mathcal{K}$ 的一个代数闭包.

定理 3.4.1 设 $\mathfrak{S}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的简单系统, 那么对任意 $1 < k \le n$ 与

$$\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\mathfrak{S}^{(k-1)})$$

都存在 $\bar{x}_k, \cdots, \bar{x}_l \in \tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}_l \in \mathrm{Zero}(\mathfrak{S}^{(l)})$ 对所有 $k \le l \le n$ 成立. 特别, $\mathfrak{S}$ 在 $\bar{\mathcal{K}}$ 上是完美的.

证 设 $\mathfrak{S} = [\mathbb{T}, \tilde{\mathbb{T}}]$, 并将 $\breve{\mathfrak{S}}$ 重排为三角列 $[T_1, \cdots, T_r]$, 其中

$$p_i = \mathrm{cls}(T_i),\ d_i = \mathrm{ldeg}(T_i),\ I_i = \mathrm{ini}(T_i),\quad 1 \le i \le r.$$

很清楚, 对任意 $k \le l$ 都存在 i 与 $s \ge 0$, 使得

$$p_{i-1} < k \le p_i,\quad p_{i+s-1} < l \le p_{i+s}.$$

设 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\mathfrak{S}^{(k-1)})$. 若 $s = 0$ 且 $l < p_i$, 则选取任意 $\bar{x}_k, \cdots, \bar{x}_l \in \mathcal{K}$. 这时, 我们有

$$\bar{\boldsymbol{x}}_l \in \mathrm{Zero}(\mathfrak{S}^{(l)}),$$

因而定理已经获证. 否则, 选取任意 $\bar{x}_k, \cdots, \bar{x}_{p_i-1} \in \mathcal{K}$. 根据定义,

$$I_i(\bar{\boldsymbol{x}}_{p_i-1}) \ne 0,\quad \text{且}\ \bar{T}_i = T_i(\bar{\boldsymbol{x}}_{p_i-1}, x_{p_i})\ \text{无平方因子}.$$

因此 $\bar{T}_i$ 关于 x_{p_i} 在 $\tilde{\mathcal{K}}$ 中有 d_i 个互异零点. 若 $T_i \in \mathbb{T}$, 则从这 d_i 个零点中任选一个作为 x_{p_i}. 若 $T_i \in \tilde{\mathbb{T}}$, 则从 $\mathcal{K}$ 中选取一个元素作为 x_{p_i}, 但该元素不是 $\bar{T}_i$ 的 d_i 个零点之一.

如果 $s = 1$ 且 $l < p_{i+1}$, 那么选取任意 $\bar{x}_{p_i+1}, \cdots, \bar{x}_l \in \mathcal{K}$, 我们有

$$\bar{\boldsymbol{x}}_l \in \mathrm{Zero}(\mathfrak{S}^{(l)}).$$

否则, 为 $x_{p_i+1}, \cdots, x_{p_{i+1}-1}$ 分别选取任意 $\bar{x}_{p_i+1}, \cdots, \bar{x}_{p_{i+1}-1} \in \mathcal{K}$. 类似地,

$$I_{i+1}(\bar{\boldsymbol{x}}_{p_{i+1}-1}) \ne 0,\quad \text{且}\ \bar{T}_{i+1} = T_{i+1}(\bar{\boldsymbol{x}}_{p_{i+1}-1}, x_{p_{i+1}})\ \text{无平方因子}.$$

与之相应, 关于 $x_{p_{i+1}}$, $\bar{T}_{i+1}$ 是次数为 d_{i+1} 的多项式, 因而在 $\tilde{\mathcal{K}}$ 中有 d_{i+1} 个互异零点.

按这种方式进行, 我们将构造出 $\mathfrak{S}^{(l)}$ 的一个零点 $\bar{\boldsymbol{x}}_l$; 由此定理获证. □

推论 3.4.2 $\mathcal{K}[\boldsymbol{x}]$ 中每个简单系统都具有强投影性质.

参阅推论 3.2.14 及有关强投影性质的定义 4.1.2. 因而 RegSer 和 SimSer 各提供了解参数代数系统的一种方法 (见定理 7.1.5 和 7.4 节).

定理 3.4.3 设 $\mathfrak{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任一多项式系统, 而 Ψ 为 $\mathfrak{P}$ 的简单序列, 那么

(a) $\mathrm{Zero}(\mathfrak{P}) = \emptyset$ 当且仅当 $\Psi = \emptyset$;

(b) $\mathrm{Zero}(\mathfrak{P})$ 为有限集当且仅当 $|\mathbb{T}| = n$ 且 $\tilde{\mathbb{T}} = \emptyset$ 对每个 $[\mathbb{T}, \tilde{\mathbb{T}}] \in \Psi$ 都成立.

证 (a) 由 (3.3.4) 和定理 3.4.1 即得.

(b) 对任意 $[\mathbb{T}, \tilde{\mathbb{T}}] \in \Psi$, 若 $|\mathbb{T}| = n$, 则 $\tilde{\mathbb{T}} = \emptyset$, 且 $\mathbb{T}$ 可写为 $[T_1, \cdots, T_n]$, 使得 $\mathrm{cls}(T_i) = i$. 令 $d_i = \mathrm{ldeg}(T_i)$, 那么 T_1 关于 x_1 在 $\tilde{\mathcal{K}}$ 中有 d_1 个互异零点, 而且对这 d_1 个零点中的任意一个, T_2 关于 x_2 在 $\tilde{\mathcal{K}}$ 中有 d_2 个互异零点, 如此等等. 因此 $\mathbb{T}$ 有 $d_1 \cdots d_n$ 个互异零点, 这些零点构成一有限集合. 若 $|\mathbb{T}| < n$, 则存在 k, 使得 $\mathbb{T}^{\langle k \rangle} = \emptyset$. 所以 x_k 在 $\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}})$ 中的取值范围在 $\tilde{\mathbb{T}}^{\langle k \rangle} = \emptyset$ 时为 $\tilde{\mathcal{K}}$; 如果 $\tilde{\mathbb{T}}^{\langle k \rangle} \neq \emptyset$, 该范围是 $\tilde{\mathcal{K}}$ 减去有限多个元素. 无论哪种情形, $\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}})$ 都是无限的. 依据 (3.3.4), (b) 获证. □

按照定理 3.4.3, 我们可以用 SimSer 来确定任意多项式方程和不等方程系统的可解性 (不需要多项式因子分解). 换句话说, 该算法给出了代数闭域上初等代数和几何判定问题的一个解答. 由上面的证明可见, 在 $\mathrm{Zero}(\mathfrak{P})$ 有限时, 零点的确切个数可按照 $\mathbb{T}$ 中多项式的导次数来计算; 所有零点可从 $\mathbb{T}$ 依次求得.

定理 3.4.4 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意简单系统 $[\mathbb{T}, \tilde{\mathbb{T}}]$ 和多项式 P,

$$\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}}) \subset \mathrm{Zero}(P) \iff \mathrm{prem}(P, \mathbb{T}) = 0.$$

证 设

$$\mathrm{prem}(P, \mathbb{T}) = 0, \quad \text{且} \quad \bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}}).$$

依据定义, 对任意 $T \in \mathbb{T}$ 有 $\mathrm{ini}(T)(\bar{\boldsymbol{x}}) \neq 0$. 于是由伪余公式 (2.1.2) 即得 $P(\bar{\boldsymbol{x}}) = 0$. 定理的 “$\Longleftarrow$” 部分获证.

现在假设 $\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}}) \subset \mathrm{Zero}(P)$. 我们希望证明

$$R = \mathrm{prem}(P, \mathbb{T}) = 0.$$

为此，令 $\mathfrak{S}=[\mathbb{T},\tilde{\mathbb{T}}]$, 并将 $\breve{\mathfrak{S}}$ 重排为三角列 $[T_1,\cdots,T_r]$. 又命

$$p_i=\operatorname{cls}(T_i),\quad d_i=\operatorname{ldeg}(T_i),\quad 1\le i\le r.$$

对任意 $\bar{\boldsymbol{x}}_{p_r-1}\in\operatorname{Zero}(\mathfrak{S}^{(p_r-1)})$ 及任意 $\bar{x}_{p_r+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 令

$$\hat{\boldsymbol{x}}_{p_r}=(\bar{\boldsymbol{x}}_{p_r-1},x_{p_r},\bar{x}_{p_r+1},\cdots,\bar{x}_n),$$

那么 $T_r(\hat{\boldsymbol{x}}_{p_r})$ 关于 x_{p_r} 有 d_r 个互异零点. 由伪余公式 (2.1.2) 可知 $\operatorname{Zero}(\mathfrak{S})\subset\operatorname{Zero}(R)$. 因此, 在 $T_r\in\mathbb{T}$ 时 $R(\hat{\boldsymbol{x}}_{p_r})$ 关于 x_{p_r} 也有 d_r 个互异零点; 而在 $T_r\in\tilde{\mathbb{T}}$ 时, $T_r(\hat{\boldsymbol{x}}_{p_r})$ 的 d_r 个零点之外的任意 $\bar{x}_{p_r}\in\tilde{\mathcal{K}}$ 都是 $R(\hat{\boldsymbol{x}}_{p_r})$ 的零点. 由于在 $T_r\in\mathbb{T}$ 时 $\deg(R,x_{p_r})<d_r$, 故 R —— 视作 x_{p_r} 的多项式 —— 的系数 R_i 必须对 $\bar{\boldsymbol{x}}_{p_r-1}\in\operatorname{Zero}(\mathfrak{S}^{(p_r-1)})$ 以及任意 $\bar{x}_{p_r+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$ 都为零. 也就是说, 对每个 i 都有 $\operatorname{Zero}(\mathfrak{S}^{(p_r-1)})\subset\operatorname{Zero}(R_i)$. 又因为 $T_{r-1}(\bar{\boldsymbol{x}}_{p_{r-1}-1},x_{p_{r-1}})$ 关于 $x_{p_{r-1}}$ 有 d_{r-1} 个互异零点, 而在 $T_{r-1}\in\mathbb{T}$ 时 $\deg(R_i,x_{p_{r-1}})<d_{r-1}$, 所以作为 $x_{p_{r-1}}$ 的多项式每个 R_i 的系数对任意

$$\bar{\boldsymbol{x}}_{p_{r-1}-1}\in\operatorname{Zero}(\mathfrak{S}^{(p_{r-1}-1)})$$

和 $\bar{x}_{p_{r-1}+1},\cdots,\bar{x}_{p_r-1},\bar{x}_{p_r+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$ 也都为零.

继续对 $T_{r-2},\cdots,T_1$ 使用这样的论证, 我们不难看出, 作为 $x_{p_1},\cdots,x_{p_r}$ 的多项式 R 的系数在其 (参) 变元被任意数值替换后都变为零. 这就意味着 $R\equiv 0$. 证毕. □

作为上述定理的推论, 我们有以下结果.

推论 3.4.5 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意简单列 $\mathbb{T}$ 和多项式 P,

$$\operatorname{Zero}(\mathbb{T}/\operatorname{ini}(\mathbb{T}))\subset\operatorname{Zero}(P)\iff\operatorname{prem}(P,\mathbb{T})=0.$$

证 由余式公式容易看出 $\operatorname{prem}(P,\mathbb{T})=0$ 蕴涵着 $\operatorname{Zero}(\mathbb{T}/\mathbb{I})\subset\operatorname{Zero}(P)$, 其中 $\mathbb{I}=\operatorname{ini}(\mathbb{T})$. 因 $\mathbb{T}$ 是简单列, 故存在 $\tilde{\mathbb{T}}$, 使得 $[\mathbb{T},\tilde{\mathbb{T}}]$ 为简单系统. 又由简单系统的定义可知

$$\operatorname{Zero}(\mathbb{T}/\tilde{\mathbb{T}})\subset\operatorname{Zero}(\mathbb{T}/\mathbb{I}).$$

所以根据定理 3.4.4, 若 $\operatorname{Zero}(\mathbb{T}/\mathbb{I})\subset\operatorname{Zero}(P)$, 则 $\operatorname{prem}(P,\mathbb{T})=0$. □

由于所有简单列都是正则的, 命题 3.2.6 和推论 3.2.7 等在 $\mathbb{T}$ 为简单列时当然成立.

定理 3.4.4 与算法 SimSer 提供了根理想成员问题的一个解答. 该定理也可以用来证明下列简单序列的性质.

定理 3.4.6 设 $[\mathbb{P},\mathbb{Q}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统，而 Ψ 为 $[\mathbb{P},\mathbb{Q}]$ 的简单序列，那么

(a) 对每个 $[\mathbb{T},\tilde{\mathbb{T}}]\in\Psi$ 都有 $\mathrm{prem}(\mathbb{P},\mathbb{T})=\{0\}$, $0\notin\mathrm{prem}(\mathbb{Q},\mathbb{T})$;

(b)

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q})=\bigcup_{[\mathbb{T},\tilde{\mathbb{T}}]\in\Psi}\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})\cup\mathbb{Q}). \tag{3.4.1}$$

证 (a) 设 $[\mathbb{T},\tilde{\mathbb{T}}]\in\Psi$, 则 $\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}})\subset\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. 因此 $\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}})\subset\mathrm{Zero}(\mathbb{P})$, 且对任意 $Q\in\mathbb{Q}$ 有 $\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}})\not\subset\mathrm{Zero}(Q)$. 所以，由定理 3.4.4 可知 $\mathrm{prem}(\mathbb{P},\mathbb{T})=\{0\}$, 且对任意 $Q\in\mathbb{Q}$ 有 $\mathrm{prem}(Q,\mathbb{T})\neq 0$.

(b) 依据已证的 (a) 和伪余公式，(3.4.1) 式的左边包含右边. 为证相反方向，设 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$, 那么存在 $[\mathbb{T},\tilde{\mathbb{T}}]\in\Psi$, 使得 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}})$. 显然，对 $\mathrm{ini}(\mathbb{T})$ 中的任意多项式 $\bar{\boldsymbol{x}}$ 都不是其零点. 所以 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})\cup\mathbb{Q})$, 即 $\bar{\boldsymbol{x}}$ 属于 (3.4.1) 式的右边. □

推论 3.4.7 多项式系统 $\mathfrak{P}$ 的任意简单序列都是 $\mathfrak{P}$ 的 W 特征序列.

定理 3.4.8 设 $\mathfrak{S}_1=[\mathbb{T}_1,\tilde{\mathbb{T}}_1]$ 和 $\mathfrak{S}_2=[\mathbb{T}_2,\tilde{\mathbb{T}}_2]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的简单系统，且 $\mathrm{Zero}(\mathfrak{S}_1)\subset\mathrm{Zero}(\mathfrak{S}_2)$,

(a) 则对所有 $T_2\in\mathbb{T}_2$ 有 $\mathrm{prem}(T_2,\mathbb{T}_1)=0$.

又对任意 $1\leq k\leq n$:

(b) 若 $\breve{\mathfrak{S}}_1^{\langle k\rangle}=\emptyset$, 则 $\breve{\mathfrak{S}}_2^{\langle k\rangle}=\emptyset$;

(c) 假定 $\tilde{\mathbb{T}}_i^{\langle k\rangle}\neq\emptyset$, 并设 $T_i\in\tilde{\mathbb{T}}_i^{\langle k\rangle}$, $i=1,2$, 那么

$$\mathrm{prem}(T_1,\mathbb{T}_1^{(k-1)}\cup[T_2])=0.$$

证 (a) 由定理 3.4.4 即得.

(b) 首先注意，对任意 $1\leq k\leq n$ 都有

$$\mathrm{Zero}(\mathfrak{S}_1^{(k)})\subset\mathrm{Zero}(\mathfrak{S}_2^{(k)}),$$

且对任意固定的 $\bar{\boldsymbol{x}}_{k-1}\in\mathrm{Zero}(\mathfrak{S}_i^{(k-1)})$, 变元 x_k 在 $\mathrm{Zero}(\mathfrak{S}_i^{(k)})$ 中的取值范围为 $\tilde{\mathcal{K}}$ 当且仅当 $\breve{\mathfrak{S}}_i^{\langle k\rangle}=\emptyset$, $i=1,2$. 所以 $\breve{\mathfrak{S}}_1^{\langle k\rangle}=\emptyset$ 蕴涵着 $\breve{\mathfrak{S}}_2^{\langle k\rangle}=\emptyset$.

(c) 命 $\mathbb{T}_1^{*(k)} = \mathbb{T}_1^{(k-1)} \cup [T_2]$, 则 $[\mathbb{T}_1^{*(k)}, \tilde{\mathbb{T}}_1^{(k-1)}]$ 为简单系统. 并且 $[\mathbb{T}_1^{*(k)}, \tilde{\mathbb{T}}_1^{(k-1)}]$, 使得 $T_1 \neq 0$ 的任意零点 —— 若存在的话 —— 也是 $\mathfrak{S}_1^{(k)}$ 的零点, 因而也是 $\mathfrak{S}_2^{(k)}$ 的零点. 该零点的存在将导致矛盾. 所以

$$\mathrm{Zero}(\mathbb{T}_1^{*(k)}/\tilde{\mathbb{T}}_1^{(k-1)}) \subset \mathrm{Zero}(T_1),$$

因而欲证的结论由 (a) 即得. □

定理 3.4.9 设 $[\mathbb{T}_1, \tilde{\mathbb{T}}_1]$ 和 $[\mathbb{T}_2, \tilde{\mathbb{T}}_2]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的简单系统, 则 $\mathrm{Zero}(\mathbb{T}_1/\tilde{\mathbb{T}}_1) = \mathrm{Zero}(\mathbb{T}_2/\tilde{\mathbb{T}}_2)$ 当且仅当 $\mathbb{T}_1 \cup \tilde{\mathbb{T}}_1$ 和 $\mathbb{T}_2 \cup \tilde{\mathbb{T}}_2$ 中的多项式能建立起一一对应, 使得对任意相对应的多项式 T_1 和 T_2 或者 $T_1 \in \mathbb{T}_1$ 而 $T_2 \in \mathbb{T}_2$, 或者 $T_1 \in \tilde{\mathbb{T}}_1$ 而 $T_2 \in \tilde{\mathbb{T}}_2$, 并且

$$\mathrm{prem}(I_2T_1 - I_1T_2, \mathbb{T}_1) = \mathrm{prem}(I_2T_1 - I_1T_2, \mathbb{T}_2) = 0,$$

其中 $I_i = \mathrm{ini}(T_i)$, $i = 1, 2$.

证 我们只需证明必要性. 首先, 对系统 $[\mathbb{T}_1, \tilde{\mathbb{T}}_1]$ 和 $[\mathbb{T}_2, \tilde{\mathbb{T}}_2]$ 其相应多项式的导元必须完全一样. 这是因为对任意固定的 $\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\mathbb{T}_1^{(k-1)}/\tilde{\mathbb{T}}_1^{(k-1)})$ 导元 x_k 在 $\mathrm{Zero}(\mathbb{T}_1^{(k)}/\tilde{\mathbb{T}}_1^{(k)})$ 中的取值范围是 $\tilde{\mathcal{K}}$ 的真子集, 而在 $\mathrm{Zero}(\mathbb{T}_2^{(k)}/\tilde{\mathbb{T}}_2^{(k)})$ 中自由变元 x_k 可以取 $\tilde{\mathcal{K}}$ 中的任意数值. 所以, 每个 $T_1 \in \mathbb{T}_1^{\langle k\rangle} \cup \tilde{\mathbb{T}}_1^{\langle k\rangle}$ 都对应于某个 $T_2 \in \mathbb{T}_2^{\langle k\rangle} \cup \tilde{\mathbb{T}}_2^{\langle k\rangle}$ $(1 \leq k \leq n)$, 反之亦然. 因此, 对任意 k 与

$$\bar{\boldsymbol{x}}_{k-1} \in \mathrm{Zero}(\mathbb{T}_1^{(k-1)}/\tilde{\mathbb{T}}_1^{(k-1)}) = \mathrm{Zero}(\mathbb{T}_2^{(k-1)}/\tilde{\mathbb{T}}_2^{(k-1)}),$$

$T_1(\bar{\boldsymbol{x}}_{k-1}, x_k)$ 和 $T_2(\bar{\boldsymbol{x}}_{k-1}, x_k)$ 都无平方因子且 (关于 x_k) 具有相同的零点集. 这就意味着

$$T_1 \in \mathbb{T}_1^{\langle k\rangle} \iff T_2 \in \mathbb{T}_2^{\langle k\rangle},$$
$$I_2(\bar{\boldsymbol{x}}_{k-1}) \cdot T_1(\bar{\boldsymbol{x}}_{k-1}, x_k) - I_1(\bar{\boldsymbol{x}}_{k-1}) \cdot T_2(\bar{\boldsymbol{x}}_{k-1}, x_k) = 0.$$

由定理 3.4.4 立即获得要证的结果. □

引理 3.4.10 从 $\mathcal{K}[\boldsymbol{x}]$ 中的任意简单系统 $\mathfrak{S}$ 可求得一约化简单系统 $\mathfrak{S}^*$, 使得 $\mathrm{Zero}(\mathfrak{S}) = \mathrm{Zero}(\mathfrak{S}^*)$.

证 按引理 2.1.4 之后的注记, 可以求得约化三角系统 $\mathfrak{S}^*$, 使得 $\mathrm{Zero}(\mathfrak{S}) = \mathrm{Zero}(\mathfrak{S}^*)$. 我们需证 $\mathfrak{S}^*$ 为简单系统. 参照引理 2.1.4 的证明以及那里的注释与记号, 且设 $\tilde{\mathbb{T}} = \mathbb{U}$, $\tilde{\mathbb{T}}^* = \mathbb{U}^*$, 则

$$\mathrm{cls}(T_i^*) = \mathrm{cls}(T_i) = p_i, \quad \mathrm{ldeg}(T_i^*) = \mathrm{ldeg}(T_i) = d_i, \quad 2 \leq i \leq r.$$

所以可将 $\breve{\mathfrak{S}}^*$ 重排为三角列，且 $T_i^*(\bar{\boldsymbol{x}}_{p_i-1}, x_{p_i})$ 和 $T_i(\bar{\boldsymbol{x}}_{p_i-1}, x_{p_i})$ 关于 x_{p_i} 具有相同的零点集，该集由 d_i 个互异零点构成；因此它们对任意

$$\bar{\boldsymbol{x}}_{p_i-1} \in \mathrm{Zero}([T_1, T_2^*, \cdots, T_{i-1}^*]/\tilde{\mathbb{T}}^{(p_i-1)})$$

及 $2 \leq i \leq r$ 都无平方因子. 类似地，对任意类为 p 的 $T \in \tilde{\mathbb{T}}$，命 $T^* = \mathrm{prem}(T, \mathbb{T}^*)$；则 $\mathrm{cls}(T^*) = p$，且 $T^*(\bar{\boldsymbol{x}}_{p-1}, x_p)$ 和 $T(\bar{\boldsymbol{x}}_{p-1}, x_p)$ 关于 x_p 具有相同的零点集，因而对任意 $\bar{\boldsymbol{x}}_{p-1} \in \mathrm{Zero}(\mathbb{T}^{*(p-1)}/\tilde{\mathbb{T}}^{(p-1)})$ 都无平方因子. 于是 $[\mathbb{T}^*, \tilde{\mathbb{T}}^*]$ 为约化简单系统. □

第四章 投影与不可约零点分解

投影是保证所求三角系统完美的另一途径. 将投影过程并入零点分解算法能计算具有投影性质的三角系统. 它与前两章中所描述的算法从理论上来讲都不需要多项式因子分解. 然而现有的因子分解程序已经相当有效, 因而可被用来提高消去算法的性能. 将多项式因子分解用于这些算法的实施是一项行之有效的策略. 本章的后一部分将阐述如何使用 (代数扩域上的) 因子分解来进一步分解三角系统以便获得更具良好性质的零点分解. 我们在论述中将用到吴文俊有关著作 (如 [95] 和 [96] 第四章) 中的材料而不再一一提及.

4.1 投　影

给定 $\mathcal{K}[x_1,\cdots,x_n]$ 中的多项式系统 $[\mathbb{P},\mathbb{Q}]$. 我们希望消去变元 $x_n,\cdots,x_{k+1}$ $(0\le k<n)$ 以得到有限多个 $\mathcal{K}[x_1,\cdots,x_k]$ 中的多项式系统 $[\mathbb{P}_1,\mathbb{Q}_1],\cdots,[\mathbb{P}_e,\mathbb{Q}_e]$, 使得

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q})\neq\emptyset \iff \bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)\neq\emptyset.$$

在 $k=0$ 时, $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})\neq\emptyset$ 当且仅当存在 i, 使得 $\mathbb{P}_i\setminus\{0\}=\emptyset$ 且 $0\notin\mathbb{Q}_i$. 同时也希望对任意

$$(\bar{x}_1,\cdots,\bar{x}_k)\in\bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$$

能求得 $\mathcal{K}$ 的某一扩域 $\tilde{\mathcal{K}}$ 中的 $\bar{x}_{k+1},\cdots,\bar{x}_n$, 使得 $(\bar{x}_1,\cdots,\bar{x}_n)\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. 仅满足这两个要求的消去程序是相对简单的. 由于我们又希望建立起所给系统与消元后的 (三角) 系统之间的零点关系, 因此本章 4.2 节中所介绍的算法显得比较复杂.

基本引理

重温 2.3 节中引进的记号 $\mathbb{P}^{(i)}$, $\mathbb{P}^{[i]}$ 和 $\mathbb{P}^{\langle i\rangle}$. 我们继续将 $x_1,\cdots,x_i$ 或 $(x_1,\cdots,x_i)$ 写成 $\boldsymbol{x}_i$, 而 $\boldsymbol{x}=\boldsymbol{x}_n$. 类似地, $\bar{\boldsymbol{x}}_i$ 代表 $\bar{x}_1,\cdots,\bar{x}_i$ 或 $(\bar{x}_1,\cdots,\bar{x}_i)$, 等等. 除非另有说明, $\tilde{\mathcal{K}}$ 总表示 $\mathcal{K}$ 的某一扩域.

对任意 $\bar{x}_1,\cdots,\bar{x}_i\in\tilde{\mathcal{K}}$, 用 $\bar{x}_1,\cdots,\bar{x}_i$ 分别替换 $\mathbb{P}$ 中多项式的变元 $x_1,\cdots,x_i$ 所得的多项式组记作 $\mathbb{P}^{\langle\bar{x},i\rangle}$. 用符号表示，即

$$\mathbb{P}^{\langle\bar{x},i\rangle}\triangleq\mathbb{P}|_{\boldsymbol{x}_i=\bar{\boldsymbol{x}}_i}=\mathbb{P}|_{x_1=\bar{x}_1,\cdots,x_i=\bar{x}_i}.$$

对任意多项式系统 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$, 我们有

$$\mathfrak{P}^{\langle\bar{x},i\rangle}\triangleq[\mathbb{P}^{\langle\bar{x},i\rangle},\mathbb{Q}^{\langle\bar{x},i\rangle}].$$

定义 4.1.1 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意多项式系统 $\mathfrak{P}$ 以及 $1\le i\le n-1$, 定义 $\mathrm{Zero}(\mathfrak{P})$ 到 $\boldsymbol{x}_i$ 的 *投影* 为

$$\mathrm{Proj}_{\boldsymbol{x}_i}\mathrm{Zero}(\mathfrak{P})\triangleq\left\{\bar{\boldsymbol{x}}_i\in\tilde{\mathcal{K}}^i:\ \begin{array}{l}\exists\bar{x}_{i+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}},\\ \text{使得 }\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathfrak{P})\end{array}\right\}.$$

此外，我们对极端情形 $i=n$ 定义

$$\mathrm{Proj}_{\boldsymbol{x}}\mathrm{Zero}(\mathfrak{P})\triangleq\mathrm{Zero}(\mathfrak{P}),$$

而对极端情形 $i=0$ 定义

$$\mathrm{Proj}\mathrm{Zero}(\mathfrak{P})\triangleq\begin{cases}\emptyset & \text{若 }\mathrm{Zero}(\mathfrak{P})=\emptyset,\\ \{0\} & \text{否则}.\end{cases}$$

容易看出

$$\mathrm{Proj}_{\boldsymbol{x}_i}\mathrm{Zero}(\mathfrak{P})\neq\emptyset\iff\mathrm{Zero}(\mathfrak{P})\neq\emptyset.$$

而且，对 i 个元素 $\bar{x}_1,\cdots,\bar{x}_i\in\tilde{\mathcal{K}}$,

$$\bar{\boldsymbol{x}}_i\in\mathrm{Proj}_{\boldsymbol{x}_i}\mathrm{Zero}(\mathfrak{P})\iff\mathrm{Zero}(\mathfrak{P}^{\langle\bar{x},i\rangle})\neq\emptyset.$$

对任意多项式系统 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$, 若 $\mathbb{P}^{[i]}=\mathbb{Q}^{[i]}=\emptyset$, 则明显有 $\mathrm{Proj}_{\boldsymbol{x}_i}\mathrm{Zero}(\mathfrak{P})=\mathrm{Zero}(\mathfrak{P})$.

引理 4.1.1 设 $[\mathbb{P},\mathbb{Q}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中级 $\le i$ 的多项式系统. 假定 $\mathbb{Q}^{[i]}\neq\emptyset$, 且设 $H_1,\cdots,H_h$ 为 $\mathbb{Q}^{[i]}$ 中的所有多项式. 用 $H_{l1},\cdots,H_{lm_l}$ 表示 H_l 以所有 $\succ x_i$ 的变元为变元的多项式之非零系数，那么

$$\mathrm{Proj}_{\boldsymbol{x}_i}\mathrm{Zero}(\mathbb{P}/\mathbb{Q})=\bigcup_{1\le j_1\le m_1,\cdots,1\le j_h\le m_h}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}_{j_1\cdots j_h}),\qquad(4.1.1)$$

$$\operatorname{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{1\le j_1\le m_1,\cdots,1\le j_h\le m_h} \operatorname{Zero}(\mathbb{P}/\mathbb{Q}'_{j_1\cdots j_h}), \tag{4.1.2}$$

其中

$$\mathbb{Q}_{j_1\cdots j_h} = \mathbb{Q}^{(i)} \cup \{H_{1j_1},\cdots,H_{hj_h}\},$$
$$\mathbb{Q}'_{j_1\cdots j_h} = \mathbb{Q} \cup \{H_{1j_1},\cdots,H_{hj_h}\}.$$

证 我们首先证明 (4.1.1). 对任意 $\bar{\boldsymbol{x}}_i \in \operatorname{Proj}_{\boldsymbol{x}_i}\operatorname{Zero}(\mathbb{P}/\mathbb{Q})$, 依据定义存在 $\bar{x}_{i+1},\cdots,\bar{x}_n \in \tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}} \in \operatorname{Zero}(\mathbb{P}/\mathbb{Q})$. 明显有 $H_l(\bar{\boldsymbol{x}}) \neq 0$, 因此对每个 l,

$$H_{l1}(\bar{\boldsymbol{x}}_i),\cdots,H_{lm_l}(\bar{\boldsymbol{x}}_i)$$

不能全为 0; 设 j'_l 为使 $H_{lj'_l}(\bar{\boldsymbol{x}}_i) \neq 0$ 的整数, 则

$$\bar{\boldsymbol{x}}_i \in \operatorname{Zero}(\mathbb{P}/\mathbb{Q}_{j'_1\cdots j'_h}). \tag{4.1.3}$$

另一方面, 如果 $\bar{\boldsymbol{x}}_i$ 属于 (4.1.1) 式的右边, 则必存在 $j'_1,\cdots,j'_h$, 使得 (4.1.3) 式成立. 因而, 对所有 l 都有

$$H_l(\bar{\boldsymbol{x}}_i, x_{i+1},\cdots,x_n) \neq 0.$$

故存在 $\bar{x}_{i+1},\cdots,\bar{x}_n \in \tilde{\mathcal{K}}$, 使得 $H_1\cdots H_h(\bar{\boldsymbol{x}}) \neq 0$. 即对所有 l 都有 $H_l(\bar{\boldsymbol{x}}) \neq 0$. 所以, $\bar{\boldsymbol{x}} \in \operatorname{Zero}(\mathbb{P}/\mathbb{Q})$; 因此 $\bar{\boldsymbol{x}}_i \in \operatorname{Proj}_{\boldsymbol{x}_i}\operatorname{Zero}(\mathbb{P}/\mathbb{Q})$.

为了证明 (4.1.2), 我们首先注意该式的左边明显包含右边. 原因是对每组 $j_1,\cdots,j_h$ 都有

$$\operatorname{Zero}(\mathbb{P}/\mathbb{Q}'_{j_1\cdots j_h}) \subset \operatorname{Zero}(\mathbb{P}/\mathbb{Q}).$$

另一方面, 对任意 $\bar{\boldsymbol{x}} \in \operatorname{Zero}(\mathbb{P}/\mathbb{Q})$ 及每个 l, 设 j'_l 为使得 $H_{lj'_l}(\bar{\boldsymbol{x}}_i) \neq 0$ 的任意整数 (如前), 那么

$$\bar{\boldsymbol{x}} \in \operatorname{Zero}(\mathbb{P}/\mathbb{Q}'_{j'_1\cdots j'_h}),$$

因此 $\bar{\boldsymbol{x}}$ 属于 (4.1.2) 式的右边. □

注 4.1.1 在引理 4.1.1 中, 可用 $\mathbb{P} \cup \mathbb{H}_{j_1\cdots j_h}$ 来替换零点关系式 (4.1.1) 和 (4.1.2) 右边的 $\mathbb{P}$ 而使其复杂化, 这里

$$\mathbb{H}_{j_1\cdots j_h} = \{H_{lj}\colon\ 0 \le j \le j_l - 1, 1 \le l \le h\} \setminus \{0\},$$

而 $H_{l0} = 0$, $l = 1,\cdots,h$. 这种复杂化具有实际意义, 道理是所考虑的系统中含多项式愈多, 消元 —— 特别是在该系统无零点时 —— 就愈容易. 这种对零点关系的修正将给出 (4.2 节中所描述的) 子算法 ProjA 的一个较复杂的版本.

引理 4.1.2 设 T 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式，且

$$\mathrm{cls}(T)=i>0,\quad \mathrm{ini}(T)=I,\quad \mathrm{ldeg}(T)=d,$$

而 $[\mathbb{P},\mathbb{Q}]$ 为级 $\ell \leq i-1$ 且 $\mathrm{level}(\mathbb{Q})\leq i$ 的多项式系统.

(a) 若 $\mathbb{Q}^{\langle i\rangle}=\emptyset$, 则对任意 $\ell\leq j\leq i-1$ 有

$$\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q}\cup\{I\})=\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}\cup\{I\}).\tag{4.1.4}$$

(b) 假定 $\mathbb{Q}^{\langle i\rangle}\neq\emptyset$, 且设 $H_1,\cdots,H_h$ 为 $\mathbb{Q}^{\langle i\rangle}$ 中的所有多项式. 又命

$$R=\mathrm{prem}((H_1\cdots H_h)^d,T),\quad \mathbb{Q}'=\mathbb{Q}^{(i-1)}\cup\{I,R\},$$

则对任意 $\ell\leq j\leq i-1$ 有

$$\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q}\cup\{I\})=\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}'),\tag{4.1.5}$$

$$\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q}\cup\{I\})=\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q}').\tag{4.1.6}$$

证 (a) 此时 $\mathbb{Q}$ 中所有多项式的类都 $<i$, 即 $\mathbb{Q}\subset\mathcal{K}[\boldsymbol{x}_{i-1}]$. (4.1.4) 式的右边明显包含其左边. 为了证明相反方向，考虑任意 $\ell\leq j\leq i-1$ 及

$$\bar{\boldsymbol{x}}_j\in\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}\cup\{I\}).$$

由定义知存在 $\bar{x}_{j+1},\cdots,\bar{x}_{i-1}\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}_{i-1}\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q}\cup\{I\})$. 依据代数基本定理，$T(\bar{\boldsymbol{x}}_{i-1},x_i)$ 关于 x_i 有一零点 $\bar{x}_i\in\tilde{\mathcal{K}}$. 因此，$\bar{\boldsymbol{x}}_i$ 属于 (4.1.4) 式的左边.

(b) 为证 (4.1.5), 首先考虑任意

$$\bar{\boldsymbol{x}}_j\in\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q}\cup\{I\}),\tag{4.1.7}$$

易知存在 $\bar{x}_{j+1},\cdots,\bar{x}_i\in\tilde{\mathcal{K}}$, 使得

$$T(\bar{\boldsymbol{x}}_i)=0,\quad I(\bar{\boldsymbol{x}}_{i-1})\neq 0,\quad H_1\cdots H_h(\bar{\boldsymbol{x}}_i)\neq 0.$$

根据伪余公式

$$I^s(H_1\cdots H_h)^d=AT+R,\tag{4.1.8}$$

其中 $s\geq 0$ 为整数，我们有 $R(\bar{\boldsymbol{x}}_i)\neq 0$. 因而，$\bar{\boldsymbol{x}}_i\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q}')$. 这就意味着

$$\bar{\boldsymbol{x}}_j\in\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}').\tag{4.1.9}$$

现假设 (4.1.9) 成立，则存在 $\bar{x}_{j+1},\cdots,\bar{x}_i\in\tilde{\mathcal{K}}$，使得 $\bar{\boldsymbol{x}}_i\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q}')$. 注意，当 $T,H_1,\cdots,H_h$ 视为 $\mathcal{K}(\boldsymbol{x}_{i-1})[x_i]$ 中的多项式时，T 有一个在所有 $H_1,\cdots,H_h$ 中都不出现的因子当且仅当 $R\neq 0$. 由于 $R(\bar{\boldsymbol{x}}_i)\neq 0$，因而 $T(\bar{\boldsymbol{x}}_{i-1},x_i)$ 必有一个因子，譬如说 T'，它不是任一 $H_l(\bar{\boldsymbol{x}}_{i-1},x_i)$ $(1\leq l\leq h)$ 的因子. 所以，在 $\mathcal{K}(\bar{\boldsymbol{x}}_{i-1})$ (因此也是 $\mathcal{K}$) 的某一代数扩域中必定存在 $\tilde{x}_i$，使得

$$T(\bar{\boldsymbol{x}}_{i-1},\tilde{x}_i)=0,\quad \text{而}\quad H_1\cdots H_h(\bar{\boldsymbol{x}}_{i-1},\tilde{x}_i)\neq 0$$

(实际上 T' 的每个零点都满足这些要求). 故有

$$(\bar{\boldsymbol{x}}_{i-1},\tilde{x}_i)\in\mathrm{Zero}(\mathbb{P}\cup\{T\}/\mathbb{Q}\cup\{I\}).$$

因此 (4.1.7) 成立，(4.1.5) 式获证.

最后，由公式 (4.1.8) 容易看出，在条件 $I\neq 0$ 之下，$H_1\cdots H_h\neq 0$ 当且仅当 $R\neq 0$. 于是 (4.1.6) 成立. □

三角系统的投影

考虑良好三角系统 $[\mathbb{T},\mathbb{U}]$，其中

$$\mathbb{T}=[T_1,\cdots,T_r].$$

设 $\mathrm{cls}(T_i)=p_i$，显然 $0<p_1<\cdots<p_r\leq n$. 一般来说，对每个 i 及任意

$$\bar{\boldsymbol{x}}_{p_i}\in\mathrm{Zero}(\mathbb{T}^{\{i\}}/\mathbb{U}^{(p_i)}),$$

不一定存在 $\bar{x}_{p_i+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$，使得 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}/\mathbb{U})$. 也就是说，

$$[\mathbb{T}^{[p_i]\langle\bar{x},p_i\rangle},\mathbb{U}^{[p_i]\langle\bar{x},p_i\rangle}]$$

不一定是完美的. 我们说明如何用引理 4.1.1 和 4.1.2 中所示的投影来处理这一情形. 这里 *投影* 是指完成下列情形 A 和 B 之一所给的任务. 首先是对 T_r 而言.

情形 A. 若 $p_r=n$，则跳过这一情形. 若 $p_r<n$ 且 $\mathbb{U}^{[p_r]}=\emptyset$，则执行下面的情形 B. 否则的话，假定 $p_r<n$ 且 $\mathbb{U}^{[p_r]}\neq\emptyset$. 设 $H_1,\cdots,H_h$ 为 $\mathbb{U}^{[p_r]}$ 中的所有多项式，并用 $H_{l1},\cdots,H_{lm_l}$ 来表示每个 H_l —— 视为变元 $\succ x_{p_r}$ 的多项式 —— 的所有 (非零) 系数，则由引理 4.1.1 得

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U})=\bigcup_{1\leq j_1\leq m_1,\cdots,1\leq j_h\leq m_h}\mathrm{Zero}(\mathbb{T}/\mathbb{U}_{j_1\cdots j_h}),\tag{4.1.10}$$

其中

$$\mathbb{U}_{j_1\cdots j_h} = \mathbb{U}\cup\{H_{1j_1},\cdots,H_{hj_h}\}.$$

为了简化记号，令

$$\mathcal{J} = \{j_1\cdots j_h\colon\ 1\le j_1\le m_1,\cdots,1\le j_h\le m_h\},$$

即 $\mathcal{J}$ 为 $\mathbb{U}_{j_1\cdots j_h}$ 的下标构成的集合，那么，对任意 $\bar{\boldsymbol{x}}_{p_r}\in \mathrm{Zero}(\mathbb{T}/\mathbb{U}^{(p_r)})$, 都存在 $\bar{x}_{p_r+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得 $H_1\cdots H_h(\bar{\boldsymbol{x}})\neq 0$, 当且仅当对某个 $j_1\cdots j_h\in\mathcal{J}$ 有

$$H_{1j_1}\cdots H_{hj_h}(\bar{\boldsymbol{x}}_{p_r})\neq 0.$$

或者等价地，我们有

$$\mathrm{Proj}_{\boldsymbol{x}_{p_r}}\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{j\in\mathcal{J}}\mathrm{Zero}(\mathbb{T}/\mathbb{U}_j^{(p_r)}).$$

情形 B. 考虑每个三角系统 $[\mathbb{T},\mathbb{U}_j]$, $j\in\mathcal{J}$, 且注意 $\mathrm{Zero}(\mathbb{T}/\mathbb{U}_j\cup\mathrm{ini}(\mathbb{T})) = \mathrm{Zero}(\mathbb{T}/\mathbb{U}_j)$. 若 $\mathbb{U}_j^{\langle p_r\rangle}=\emptyset$, 则按引理 4.1.2 (a) 有

$$\mathrm{Proj}_{\boldsymbol{x}_{p_r-1}}\mathrm{Zero}(\mathbb{T}/\mathbb{U}_j) = \mathrm{Zero}(\mathbb{T}^{\{r-1\}}/\mathbb{U}_j^{(p_r-1)}).$$

在这一情形，对 T_{r-1} 执行下一步.

否则，设 $K_1,\cdots,K_k$ 为 $\mathbb{U}_j^{\langle p_r\rangle}$ 中的所有多项式，计算

$$R = \mathrm{prem}((K_1\cdots K_k)^{\mathrm{ldeg}(T_r)},T_r),\quad \mathbb{U}_j' = \mathbb{U}_j\setminus\mathbb{U}_j^{\langle p_r\rangle}\cup\{R\}.$$

若 $R=0$, 则 $\mathrm{Zero}(\mathbb{T}/\mathbb{U}_j)=\emptyset$, 因而将三角系统 $[\mathbb{T},\mathbb{U}_j]$ 抹去. 在 $R\neq 0$ 的情形，应用引理 4.1.2 (b) 得

$$\begin{aligned}&\mathrm{Proj}_{\boldsymbol{x}_{p_r-1}}\mathrm{Zero}(\mathbb{T}/\mathbb{U}_j) = \mathrm{Proj}_{\boldsymbol{x}_{p_r-1}}\mathrm{Zero}(\mathbb{T}^{\{r-1\}}/\mathbb{U}_j'^{(p_r)}),\\ &\mathrm{Zero}(\mathbb{T}/\mathbb{U}_j) = \mathrm{Zero}(\mathbb{T}/\mathbb{U}_j').\end{aligned}\tag{4.1.11}$$

将 (4.1.10) 和 (4.1.11) 式结合起来即得

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{j\in\mathcal{J}}\mathrm{Zero}(\mathbb{T}/\mathbb{U}_j').$$

同时，我们又有

$$\mathrm{Proj}_{\boldsymbol{x}_{p_{r-1}}}\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{j\in\mathcal{J}}\mathrm{Proj}_{\boldsymbol{x}_{p_{r-1}}}\mathrm{Zero}(\mathbb{T}^{\{r-1\}}/\mathbb{U}_j'^{(p_r)}).$$

上面的投影情形 A 和 B 可就 T_{r-1} 而言对每个三角系统 $[\mathbb{T}^{\{r-1\}}, \mathbb{U}_j^{\prime(p_r)}]$ 重复，并如此进行下去. 按照这种方式，或者所有被分裂的三角系统都被抹去因而 $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \emptyset$, 或者最终获得有限多个多项式组 $\mathbb{U}_1^*, \cdots, \mathbb{U}_s^*$, 使得

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{s} \mathrm{Zero}(\mathbb{T}/\mathbb{U}_i^*). \tag{4.1.12}$$

特别在仅对 $x_n, \cdots, x_{k+1}$ 需要投影时，设 t 为使得 $p_t < k+1 \leq p_{t+1}$ 的整数，那么，投影就 $T_r, \cdots, T_{t+1}$ 而言首先对情形 A 和 B 进行，而最后再对情形 A 在 $p = k$ 时进行. 由此可得

$$\mathrm{Proj}_{\boldsymbol{x}_k} \mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{s} \mathrm{Zero}(\mathbb{T}^{(k)}/\mathbb{U}_i^{*(k)}).$$

定义 4.1.2 设 $\mathfrak{T} = [\mathbb{T}, \mathbb{U}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的良好三角系统，而 k 为非负整数. 称 $\mathfrak{T}$ 具有

- k 维 *投影性质*, 如果

$$\mathrm{Zero}(\mathfrak{T}^{(i)}) \subset \mathrm{Proj}_{\boldsymbol{x}_i} \mathrm{Zero}(\mathfrak{T}) \tag{4.1.13}$$

  对 $i = k$ 及所有 $i \in \{\mathrm{cls}(T):\ T \in \mathbb{T}, \mathrm{cls}(T) > k\}$ 成立;

- k 维 *强投影性质*, 如果 (4.1.13) 对所有 $k \leq i < n$ 成立.

  在未提及维数时，意指 $k = 0$.

引理 4.1.1 和 4.1.2 保证了以上求得的三角系统 $[\mathbb{T}, \mathbb{U}_i^*]$ $(1 \leq i \leq s)$ 都具有 k 维投影性质.

我们不再将上述关于三角系统的投影程序写成算法的形式. 该程序是 4.2 节中算法 TriSerP 的特殊情形. 这里情形 A 的设计使得投影对所有变元 $x_n, \cdots, x_{p_r+1}$ 一次进行. 这主要是基于实际考虑. 当然可以对程序作适当修改以便每次只对一个变元投影 (见注 4.2.1).

对任一多项式系统 $\mathfrak{P}$, 可用 CharSer, TriSer 或 TriSerS 计算 $\mathfrak{P}$ 的良好三角序列 Ψ. 若 $\Psi = \emptyset$, 则 $\mathrm{Zero}(\mathfrak{P}) = \emptyset$. 否则，对每个 $\mathfrak{T} = [\mathbb{T}, \mathbb{U}] \in \Psi$ 可对 $x_n, \cdots, x_{k+1}$ 投影以确定相应于 (4.1.12) 中 $\mathbb{U}_i^*$ 的多项式组. 若 $\mathrm{Zero}(\mathfrak{T}) = \emptyset$, 这一情形将在投影过程中被发现. 因此，或者对所有 $\mathfrak{T} \in \Psi$, $\mathrm{Zero}(\mathfrak{T}) = \emptyset$ 被发现，或者最终获得零点分解

$$\mathrm{Zero}(\mathfrak{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathfrak{T}_i),$$

使得

$$\mathrm{Proj}_{\boldsymbol{x}_k}\mathrm{Zero}(\mathfrak{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathfrak{T}_i^{(k)}),$$

而且每个 $\mathfrak{T}_i$ 都是具有 k 维投影性质的良好三角系统. 事实上, 对任意 $\bar{\boldsymbol{x}}_k \in \mathrm{Zero}(\mathfrak{T}_i^{(k)})$, $\mathfrak{T}_i^{[k]\langle\bar{x},k\rangle}$ 关于 $x_{k+1},\cdots,x_n$ 的零点可从该三角系统依次求得. 作为推论, 我们有 $\mathrm{Zero}(\mathfrak{P}^{\langle\bar{x},k\rangle}) \neq \emptyset$. 因而, 我们在本节开始时所提出的要求都已得到满足. 特别在 $k=0$ 时, $\mathrm{Zero}(\mathfrak{P}) = \emptyset$ 当且仅当 $e=0$.

例 4.1.1 考虑三角列 $\mathbb{T}_1 = [T_1, T_2, T_3]$, 其中

$$\begin{aligned}
T_1 &= z^3 - z^2 + r^2 - 1,\\
T_2 &= x^4 + z^2x^2 - r^2x^2 + z^4 - 2\,z^2 + 1,\\
T_3 &= xy + z^2 - 1.
\end{aligned}$$

这些多项式已在例 2.4.1 中出现. 我们希望对 $[\mathbb{T}_1, \{x\}]$ 投影; 此时设 $k=0$. 就 T_3 而言投影是不需要的. 为了对 T_2 作投影, 计算

$$R = \mathrm{prem}(x^4, T_2) = R_1x^2 + R_2,$$

其中 $R_1 = -z^2 + r^2$, $R_2 = -z^4 + 2\,z^2 - 1$. 因此, $[\mathbb{T}_1, \{x\}]$ 分裂为

$$[\mathbb{T}_1, \{R_1, R\}], \quad [\mathbb{T}_1, \{R_2, R\}].$$

为了对 T_1 投影, 我们需要计算

$$\begin{aligned}
R_1^* &= \mathrm{prem}(R_1^3, T_1)\\
&\quad = (-3\,r^4 + 5\,r^2 - 3)\,z^2 - (3\,r^4 - 4\,r^2 + 1)\,z + r^6 - 4\,r^4 + 6\,r^2 - 2,\\
R_2^* &= \mathrm{prem}(R_2^3, T_1)\\
&\quad = (-8\,r^2 + 4\,r^6 - 6\,r^4 + 11)\,z^2 - (12\,r^4 - 29\,r^2 + 17)\,z\\
&\qquad - r^8 - 4\,r^6 + 16\,r^4 - 11\,r^2 - 1.
\end{aligned}$$

分别用 R_1^* 和 R_2^* 替换两个三角系统中的 R_1 和 R_2, 我们得到

$$\mathfrak{T}_1 = [\mathbb{T}_1, \{R_1^*, R\}], \quad \mathfrak{T}_2 = [\mathbb{T}_1, \{R_2^*, R\}].$$

由于 R_i^* 关于 r 和 z 的所有系数都是常数, 无需对 $\mathfrak{T}_i$ 进一步分裂. 所以

$$\mathrm{Zero}(\mathbb{T}_1/x) = \mathrm{Zero}(\mathfrak{T}_1) \cup \mathrm{Zero}(\mathfrak{T}_2),$$

且每个 $\mathfrak{T}_i$ 都具有投影性质. 特别对任意 $(\bar{r},\bar{z}) \in \mathrm{Zero}(T_1/R_i^*)$ 有

$$\mathrm{Zero}([\bar{T}_2,\bar{T}_3]/x) \neq \emptyset,$$

这里 $\bar{T}_i = T_i|_{r=\bar{r},z=\bar{z}}$, $i=1,2,3$. 然而, 原来的 $[\mathbb{T}_1,\{x\}]$ 并不满足这一性质. 这一点通过取值 $\bar{r}=\bar{z}=1$ 容易看出, 此时

$$\bar{T}_1 = R_1^*|_{r=\bar{r},z=\bar{z}} = R_2^*|_{r=\bar{r},z=\bar{z}} = 0, \quad \bar{T}_2 = x^3, \quad \bar{T}_3 = xy.$$

因而 $(1,1) \in \mathrm{Zero}(T_1)$, 但 $(1,1) \notin \mathrm{Zero}(T_1/R_i^*)$. 现在

$$\mathrm{Zero}([\bar{T}_2,\bar{T}_3]/x) = \emptyset.$$

最后, 我们注意例 2.4.1 中 $\mathfrak{T}_3 = [\mathbb{T}_2,\emptyset]$ 的投影不改变该三角系统. 所以, 那里给出的多项式组 $\mathbb{P}$ 可分解为三个三角系统 $\mathfrak{T}_1,\mathfrak{T}_2,\mathfrak{T}_3$, 使得

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{3} \mathrm{Zero}(\mathfrak{T}_i),$$

而且每个 $\mathfrak{T}_i$ 都具有投影性质.

参见注 4.1.1 和其中定义的 $\mathbb{H}_{j_1\cdots j_h}$. 如果将那里所示的修正并入上述对 $[\mathbb{T},\mathbb{U}]$ 的投影过程, 那么在相应的地方 $\mathbb{T}$ 应由 $\mathbb{T}\cup\mathbb{H}_j$ $(j\in\mathcal{J})$ 来替代. 这时, 我们得到吴文俊投影方法[103]. 一般来说, $\mathbb{T}\cup\mathbb{H}_j$ 不再是三角列, 因而其三角序列需要进一步计算. 鉴于这一原因, 高小山和周咸青在文献 [25] 中也丢弃了 $\mathbb{H}_j$.

在 $\mathbb{U}_j^{\langle p_r\rangle} \neq \emptyset$ 时, 投影情形 B 明显耗时. 原因是伪余式

$$\mathrm{prem}\left(\prod_{K\in\mathbb{U}_j^{\langle p_r\rangle}} K^{\mathrm{ldeg}(T_r)}, T_r\right)$$

难以计算. 这一投影过程可以通过计算最大公因子和正则化来消去 $\mathbb{U}_j^{\langle p_r\rangle}$ 中的多项式而得以改进.

我们将在下节中说明如何将上述投影过程有效地嵌入算法 TriSer 中以便在投影之前不需计算三角序列.

4.2 带投影的零点分解

参见 2.3 节中引进的三元组数据结构. 我们现在定义四元组以帮助理解本节中介绍的算法.

数据结构 级为 i $(1 \leq i \leq n)$ 的 *四元组* 是由四个元素构成的表 $[\mathbb{P},\mathbb{Q},\mathbb{T},\mathbb{U}]$, 使得 $[\mathbb{P},\mathbb{Q},\mathbb{T}]$ 为三元组, $\operatorname{level}(\mathbb{Q}) = q \leq p$, 而 $\mathbb{U}$ 是 $\mathcal{K}[\boldsymbol{x}]$ 中满足 $\mathbb{U}^{(q)} = \emptyset$ 的多项式组, 这里

$$p = \begin{cases} \operatorname{cls}(\operatorname{op}(1,\mathbb{T})) & \text{若 } \mathbb{T} \neq \emptyset, \\ n & \text{否则}. \end{cases} \tag{4.2.1}$$

对任意多项式系统 $[\mathbb{P},\mathbb{Q}]$, 可对某个 i 及 q 将 $\mathbb{P}$ 和 $\mathbb{Q}$ 写为

$$\mathbb{P} = \mathbb{P}^{(i)} \cup \mathbb{P}^{[i]}, \quad \mathbb{Q} = \mathbb{Q}^{(q)} \cup \mathbb{Q}^{[q]},$$

使得 $\operatorname{level}(\mathbb{P}^{(i)}) = i$, $\mathbb{P}^{[i]}$ 能排成三角列 $\mathbb{T}$, 而 $q = \operatorname{level}(\mathbb{Q}^{(q)}) \leq p$, 其中 p 由 (4.2.1) 式定义. 置 $\mathbb{U} = \mathbb{Q}^{[q]}$, 则 $[\mathbb{P}^{(i)},\mathbb{Q}^{(q)},\mathbb{T},\mathbb{U}]$ 为四元组, 对此我们所关心的是 $\operatorname{Zero}(\mathbb{P}^{(i)} \cup \mathbb{T}/\mathbb{Q}^{(q)} \cup \mathbb{U})$.

下面的子算法 ProjA 实施了引理 4.1.1. 通过投影多项式系统 $[\mathbb{P},\mathbb{Q}]$ 分裂为有限多个子系统, 其中之一作为 $[\mathbb{P},\mathbb{Q}',\mathbb{T},\mathbb{U}']$ (在步骤 P2.4 中) 被分离出来, 而其他子系统则被搁入 Θ. 对应于引理 4.1.1 中 $H_1,\cdots,H_h$ 的那些多项式从 $\mathbb{Q}$ 中移至 $\mathbb{U}$, 构成输出集 $\mathbb{Q}'$ 和 $\mathbb{U}'$ (步骤 P1).

算法 ProjA: $[\mathbb{Q}',\mathbb{U}',\Theta] \leftarrow \operatorname{ProjA}(\mathbb{P},\mathbb{Q},\mathbb{T},\mathbb{U},i)$. 任给整数 $i > 0$ 和级为 i 的四元组 $[\mathbb{P},\mathbb{Q},\mathbb{T},\mathbb{U}]$, 本算法计算级 $\leq i$ 的多项式组 $\mathbb{Q}'$, 多项式组 $\mathbb{U}' = \mathbb{U} \cup \mathbb{Q}^{[i]}$ 和级为 i 的四元组的集合 Θ 使得

$$\operatorname{Proj}_{\boldsymbol{x}_i}\operatorname{Zero}(\mathbb{P}/\mathbb{Q}) = \operatorname{Zero}(\mathbb{P}/\mathbb{Q}') \cup \bigcup_{[\mathbb{P},\mathbb{Q}^*,\mathbb{T},\mathbb{U}'] \in \Theta} \operatorname{Zero}(\mathbb{P}/\mathbb{Q}^*), \tag{4.2.2}$$

$$\operatorname{Zero}(\mathbb{P}/\mathbb{Q}) = \operatorname{Zero}(\mathbb{P}/\mathbb{Q}' \cup \mathbb{Q}^{[i]}) \cup \bigcup_{[\mathbb{P},\mathbb{Q}^*,\mathbb{T},\mathbb{U}'] \in \Theta} \operatorname{Zero}(\mathbb{P}/\mathbb{Q}^* \cup \mathbb{Q}^{[i]}), \tag{4.2.3}$$

这里 $\operatorname{level}(\mathbb{Q}^*) \leq i$.

P1. 命 $\mathbb{Q}' \leftarrow \mathbb{Q}^{(i)}$, $\mathbb{U}' \leftarrow \mathbb{U} \cup \mathbb{Q}^{[i]}$, $\Theta \leftarrow \emptyset$.

P2. 若 $\mathbb{Q}^{[i]} \neq \emptyset$, 则:

P2.1. 设 $H_1,\cdots,H_h$ 为 $\mathbb{Q}^{[i]}$ 中的所有多项式.

P2.2. 对 $l=1,\cdots,h$ 执行下列步骤:

P2.2.1. 计算 $V_l \leftarrow \{x_j\colon \deg(H_l,x_j)>0, i<j\le n\}$.

P2.2.2. 设 $\mathcal{H}_l$ 为 H_l 关于 V_l 的所有非零系数构成的集合. 若 $\mathcal{H}_l \cap \mathcal{K} \neq \emptyset$, 则命 $m_l \leftarrow 1, H_{l1} \leftarrow 1$; 否则, 设 $H_{l1},\cdots,H_{lm_l}$ 为 $\mathcal{H}_l$ 中的所有多项式.

P2.3. 构造集合

$$\Theta \leftarrow \left\{[\mathbb{P},\mathbb{Q}' \cup \{H_{1j_1},\cdots,H_{hj_h}\},\mathbb{T},\mathbb{U}']\colon \begin{array}{l} 1\le j_1\le m_1,\cdots, \\ 1\le j_h \le m_h \end{array}\right\}.$$

P2.4. 命 $\mathbb{Q}' \leftarrow \mathbb{Q}' \cup \{H_{11},\cdots,H_{h1}\}$, $\Theta \leftarrow \Theta \setminus \{[\mathbb{P},\mathbb{Q}',\mathbb{T},\mathbb{U}']\}$.

证　本算法不带有无限循环, 因此其终止性是显然的.

为证 (4.2.2) 和 (4.2.3), 我们首先注意, 在步骤 P2.2.2 中若 $\mathcal{H}_l \cap \mathcal{K} \neq \emptyset$, 则 H_l 至少有一项系数为非零常数. 此时, 对任意 $\bar{\boldsymbol{x}}_i \in \tilde{\mathcal{K}}^i$ 总存在 $\bar{x}_{i+1},\cdots,\bar{x}_n \in \tilde{\mathcal{K}}$, 使得 $H_l(\bar{\boldsymbol{x}}) \neq 0$. 所以我们不必考虑 H_l 关于 V_l 的系数. 换言之, H_l 是不必要的. 这一情形可以通过简单地选取 $m_l=1$ 和 $H_{l1}=1$ 来加以处理.

除了上述细微的修改, 这里的 $[\mathbb{P},\mathbb{Q}']$ 与引理 4.1.1 中以 $j_1=1,\cdots,j_h=1$ 为下标的子系统相对应, 而被搁入 Θ 中的 $[\mathbb{P},\mathbb{Q}^*]$ 则对应于引理 4.1.1 中所有其他下标的子系统. 所以 (4.2.2) 和 (4.2.3) 只不过是引理 4.1.1 中 (4.1.1) 和 (4.1.2) 式的变形. □

现在我们来介绍带投影的消去算法. 该算法是通过对 TriSer 作如下修改所得: (i) 用投影情形 B 的步骤 T2.2.4 (此时有类为 i 的多项式但无类 $>i$ 的多项式需要 "投影") 来替换 PriTriSys 中的约化步骤 P2.3; (ii) 插入投影情形 A 的步骤 T2.2.3 和 T2.3 (此时有类 $>i$ 的多项式需要 "投影").

算法 TriSerP: $\Psi \leftarrow \mathrm{TriSerP}(\mathbb{P},\mathbb{Q},k)$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P},\mathbb{Q}]$ 和整数 k $(0\le k<n)$, 本算法或者求得空集 Ψ 因而表明 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})=\emptyset$, 或者计算出一个有限非空集合

$$\Psi=\{[\mathbb{P}_1,\mathbb{Q}_1,\mathbb{T}_1,\mathbb{U}_1],\cdots,[\mathbb{P}_e,\mathbb{Q}_e,\mathbb{T}_e,\mathbb{U}_e]\},$$

其中每个 $[\mathbb{P}_i,\mathbb{Q}_i,\mathbb{T}_i,\mathbb{U}_i]$ 都是级 $\le k$ 且 $\mathrm{level}(\mathbb{Q}_i)\le k$ 的四元组, 使得

(a)

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q})=\bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{P}_i\cup\mathbb{T}_i/\mathbb{Q}_i\cup\mathbb{U}_i); \tag{4.2.4}$$

(b)

$$\mathrm{Proj}_{x_k}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i); \tag{4.2.5}$$

(c) 对任意 $1 \le i \le e$ 及

$j \in \{k\} \cup \{\mathrm{cls}(T):\ T \in \mathbb{T}_i\}$, $(\bar{x}_1, \cdots, \bar{x}_j) \in \mathrm{Zero}(\mathbb{P}_i \cup \mathbb{T}_i^{(j)}/\mathbb{Q}_i \cup \mathbb{U}_i^{(j)})$,

$[\mathbb{T}_i^{[j]\langle\bar{x},j\rangle}, \mathbb{U}_i^{[j]\langle\bar{x},j\rangle}]$ 都是完美三角系统，因而 $[\mathbb{T}_i, \mathbb{U}_i]$ 也是.

T1. 命 $\Psi \leftarrow \emptyset$, $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, \emptyset, \emptyset]\}$.

T2. 重复下列步骤直至 $\Phi = \emptyset$:

T2.1. 设 $[\mathbb{F}, \mathbb{G}, \mathbb{T}, \mathbb{U}]$ 为 Φ 中的元素，且命

$$\Phi \leftarrow \Phi \setminus \{[\mathbb{F}, \mathbb{G}, \mathbb{T}, \mathbb{U}]\}, \quad \ell \leftarrow \mathrm{level}(\mathbb{F}).$$

T2.2. 对 $\imath = \ell, \cdots, k+1$ 执行下列步骤:

T2.2.1. 若 $\mathbb{F} \cap \mathcal{K} \setminus \{0\} \ne \emptyset$, 则转回 T2. 若 $\mathrm{level}(\mathbb{F}) < \imath$, 则转至 T2.2 对下一个 $\imath$ 执行.

T2.2.2. 计算 $[T, \mathbb{F}, \mathbb{G}, \Delta] \leftarrow \mathrm{Elim}(\mathbb{F}, \mathbb{G}, \imath)$, 且命

$$\Phi \leftarrow \Phi \cup \{\delta \cup [\mathbb{T}, \mathbb{U}]:\ \delta \in \Delta\}.$$

T2.2.3. 计算

$$[\mathbb{G}, \mathbb{U}, \Theta] \leftarrow \mathrm{ProjA}(\mathbb{F} \cup \{T\}, \mathbb{G}, \mathbb{T}, \mathbb{U}, \imath),$$

且命 $\Phi \leftarrow \Phi \cup \Theta$.

T2.2.4. 若 $\mathbb{G}^{[\imath-1]} \ne \emptyset$, 则计算

$$\mathbb{G} \leftarrow \mathbb{G}^{(\imath-1)} \cup \left\{ \mathrm{prem}\left(\prod_{G \in \mathbb{G}^{[\imath-1]}} G^{\mathrm{ldeg}(T)}, T \right) \right\}.$$

T2.2.5. 若 $0 \in \mathbb{G}$, 则转至 T2; 否则，命 $\mathbb{T} \leftarrow [T] \cup \mathbb{T}$.

T2.3. 计算

$$[\mathbb{G}, \mathbb{U}, \Theta] \leftarrow \mathrm{ProjA}(\mathbb{F}, \mathbb{G}, \mathbb{T}, \mathbb{U}, k),$$

且命 $\Phi \leftarrow \Phi \cup \Theta$.

T2.4. 命 $\Psi \leftarrow \Psi \cup \{[\mathbb{F},\mathbb{G},\mathbb{T},\mathbb{U}]\}$.

我们可以假定对每个 $\psi_i = [\mathbb{P}_i,\mathbb{Q}_i,\mathbb{T}_i,\mathbb{U}_i] \in \Psi$ 都有 $\mathbb{P}_i \cap \mathcal{K} \setminus \{0\} = \emptyset$ 和 $0 \notin \mathbb{Q}_i$. 否则, $\text{Zero}(\mathbb{P}_i \cup \mathbb{T}_i/\mathbb{Q}_i \cup \mathbb{U}_i) = \emptyset$, 因而 ψ_i 可从 Ψ 中抹去. 若 $k=0$, 则 $\text{Zero}(\mathbb{P}/\mathbb{Q}) \neq \emptyset$ 当且仅当 $e \geq 1$. 所以, 在 $k=0$ 且 $e \geq 1$ 时, $\mathbb{P}_i \setminus \{0\} = \emptyset$, 而且对所有 $1 \leq i \leq e$, $[\mathbb{T}_i,\mathbb{U}_i]$ 都具有投影性质.

例 4.2.1 见例 2.3.2. 今设 $k=0$, 并进行带投影的消元. 对 $z \in \mathbb{U}_1$, 我们需要在步骤 T2.2.4 中计算 z^5 —— 而不是 z —— 对 R_3 的伪余式. 该伪余式为 $-t^4 \rightsquigarrow t$, 因而 $\mathbb{U}_1$ 被 $\{t, t^3-1\}$ 所替代. 类似地, 对 $z \in \mathbb{U}_3$ 我们需要计算 z^5 对 R_3 的伪余式, 该伪余式为 $-t^4 \rightsquigarrow t$, 以及 t^3 对 t^3-1 的伪余式, 该伪余式为常数 1. 所以 $\mathbb{U}_3$ 被化简为 $\emptyset$. 投影步骤 T2.2.3 和 T2.3 的执行对这个特例是平凡的.

TriSerP 的证明　终止性. 对任意多项式系统 $[\mathbb{P},\mathbb{Q}]$, 定义指标三元组

$$\text{Index}(\mathbb{P}/\mathbb{Q}) \triangleq \langle d, \ell, p\rangle,$$

其中

$$\begin{aligned} d &= \min\{\deg(P,x_\ell):\ P \in \mathbb{P}^{\langle \ell\rangle}\},\\ \ell &= \text{level}(\mathbb{P}),\\ p &= \max(\ell, \text{level}(\mathbb{Q})). \end{aligned}$$

我们将两个三元组排序为 $\langle d_1,\ell_1,p_1\rangle \prec \langle d_2,\ell_2,p_2\rangle$, 如果

$$\begin{aligned} &p_1 < p_2;\ \text{或}\\ &p_1 = p_2\ \text{而}\ \ell_1 < \ell_2;\ \text{或}\\ &p_1 = p_2, \ell_1 = \ell_2\ \text{而}\ d_1 < d_2. \end{aligned}$$

对于在 TriSerP 的步骤 T2.1 中从 Ψ 中选取的四元组 ψ, 设 $\mathbb{F},\mathbb{G}$ 为 ψ 的头两个分量, 而 $\mathbb{P}^*,\mathbb{Q}^*$ 是 Δ 中某个由 Elim 从 ψ 生成的多项式系统的两个分量, 或者是 Θ 中某个由 ProjA 从 ψ 生成的四元组的头两个分量, 那么我们总有

$$\text{Index}(\mathbb{P}^*/\mathbb{Q}^*) \prec \text{Index}(\mathbb{F}/\mathbb{G}).$$

由于三元组 Index($\mathbb{P}/\mathbb{Q}$) 的每个分量都是正整数, 任意严格下降的指标三元组序列都是有限的. 所以 TriSerP 的“直至”循环只能重复有限多次. 终止性获证.

正确性. 即证明所计算的 Ψ 满足 TriSerP 中列出的性质 (a), (b) 和 (c).

(a) 与 TriSer 类似, 算法 TriSerP 也可被视为计算一多枝树 $\mathcal{T}$. 与 $\mathcal{T}$ 的根相连接的是四元组 $[\mathbb{P},\mathbb{Q},\emptyset,\emptyset]$, 而与每个节点或树叶 i 相连接的是四元组 $[\mathbb{P}_i,\mathbb{Q}_i,\mathbb{T}_i,\mathbb{U}_i]$, 使得在执行 TriSerP 的每步之后零点关系 (2.3.6), 在其右边的 $\mathbb{Q}_i$ 被 $\mathbb{Q}_i\cup\mathbb{U}_i$ 替代后, 仍然成立. 为了看出这一点, 我们只需注意在目前的情形, 树的分支同时由子算法 ProjA 所生成并保持零点关系 (4.2.3) 成立, 而 (4.2.3) 式蕴涵着

$$\mathrm{Zero}(\mathbb{P}\cup\mathbb{T}/\mathbb{Q}\cup\mathbb{U})=\mathrm{Zero}(\mathbb{P}\cup\mathbb{T}/\mathbb{G}\cup\mathbb{U})\cup\bigcup_{[\mathbb{P},\mathbb{Q}^*,\mathbb{T},\mathbb{U}]\in\Theta}\mathrm{Zero}(\mathbb{P}\cup\mathbb{T}/\mathbb{Q}^*\cup\mathbb{U}'),$$

其中 $\mathbb{U}'=\mathbb{U}\cup\mathbb{Q}^{[i]}$. 在执行步骤 T2.2.4 时, 零点集 $\mathrm{Zero}(\mathbb{F}\cup\{T\}\cup\mathbb{T}/\mathbb{G}\cup\mathbb{U})$ 也保持不变.

剪除 $\mathcal{T}$ 上 $\mathbb{P}_i$ 含有非零常数或 $0\in\mathbb{Q}_i$ 的那些叶子 i 并假定不是所有树叶都被剪去, 我们即获得零点分解 (4.2.4). 从 TriSer 的正确性证明可见, 这里的 $[\mathbb{T}_i,\mathbb{U}_i]$ 也都是三角系统.

(b) 先假设 $\bar{\boldsymbol{x}}_k\in\tilde{\mathcal{K}}^k$ 属于 (4.2.5) 式的右边, 那么存在 i, 使得 $\bar{\boldsymbol{x}}_k\in\mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$. 依据将要证明的性质 (c), 存在 $\bar{x}_{k+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得

$$(\bar{x}_{k+1},\cdots,\bar{x}_n)\in\mathrm{Zero}(\mathbb{T}_i^{\langle\bar{x},k\rangle}/\mathbb{U}_i^{\langle\bar{x},k\rangle}).$$

所以

$$\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}_i\cup\mathbb{T}_i/\mathbb{Q}_i\cup\mathbb{U}_i).\tag{4.2.6}$$

由 (4.2.4), $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$, 因而

$$\bar{\boldsymbol{x}}_k\in\mathrm{Proj}_{\boldsymbol{x}_k}\mathrm{Zero}(\mathbb{P}/\mathbb{Q}).\tag{4.2.7}$$

现假设 (4.2.7) 成立, 因此存在 $\bar{x}_{k+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. 由 (4.2.4), 必存在 i, 使得 (4.2.6) 式成立. 特别

$$\bar{\boldsymbol{x}}_k\in\mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)\subset\bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i).$$

于是 (4.2.5) 式获证.

(c) 设 $\mathbb{F},\mathbb{G},\mathbb{T},\mathbb{U}$ 和 T 与 TriSerP 中相同. 我们先证明两个断言:

(A) 如果对某个 $\imath$ 执行步骤 T2.2.3, 那么在执行之后, 对任意 $(\bar{x}_1,\cdots,\bar{x}_\imath)$ $\in \mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G})$ 有

$$\mathrm{Zero}(\mathbb{T}^{\langle\bar{x},\imath\rangle}/\mathbb{U}^{\langle\bar{x},\imath\rangle}) \neq \emptyset; \tag{4.2.8}$$

(B) 如果对某个 $\imath$ 执行步骤 T2.2.4, 那么在执行之后, 对任意 j, $\mathrm{level}(\mathbb{F}) \leq j \leq \imath-1$, 和 $(\bar{x}_1,\cdots,\bar{x}_j)\in \mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{F}/\mathbb{G})$ 有

$$\mathrm{Zero}([T]\cup\mathbb{T}^{\langle\bar{x},j\rangle}/\mathbb{U}^{\langle\bar{x},j\rangle}) \neq \emptyset. \tag{4.2.9}$$

若 $0\in\mathbb{G}$, 则 $\mathrm{Zero}(\mathbb{F}/\mathbb{G})=\emptyset$. 此时，上述性质是平凡的因而不必考虑.

为了避免记号上的混淆，下面的四元组 $[\mathbb{F},\mathbb{G},\mathbb{T},\mathbb{U}]$ 总是指其在所讨论的步骤执行之前，而相应的分量在执行之后，若改变了，则被打上星号 *. 断言的证明是对 $|\mathbb{T}|$ 使用归纳法.

情形 (i). $\mathbb{T}=\emptyset$.

(A) 设 ψ 和 ψ^* 分别为对应于 TriSerP 中的 $[\mathbb{F},\mathbb{G},\mathbb{T},\mathbb{U}]$ 在执行步骤 T2.2.3 之前和之后的四元组，那么

$$\psi=[\mathbb{F},\mathbb{G},\emptyset,\emptyset],\quad \psi^*=[\mathbb{F},\mathbb{G}^*,\emptyset,\mathbb{U}^*],$$

其中 $\mathbb{U}^*=\mathbb{G}^{[\imath]}$. 设 $\bar{\boldsymbol{x}}_\imath\in\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G}^*)$. 由 (4.2.2), 存在 $\bar{x}_{\imath+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得

$$\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G}).$$

由于 $\mathbb{U}^*\subset\mathbb{G}$, 对任意 $U\in\mathbb{U}^*$ 有 $U(\bar{\boldsymbol{x}})\neq 0$, 所以 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\emptyset/\mathbb{U}^*)$, 因而 (4.2.8) 式成立.

(B) 现对步骤 T2.2.4 而言，我们有

$$\psi=[\mathbb{F},\mathbb{G},\emptyset,\mathbb{U}],\quad \psi^*=[\mathbb{F},\mathbb{G}^*,\emptyset,\mathbb{U}],$$

其中

$$\mathbb{G}^*=\begin{cases}\mathbb{G}^{(\imath-1)}\cup\{\mathrm{prem}(\prod_{G\in\mathbb{G}^{[\imath-1]}}G^{\mathrm{ldeg}(T)},T)\} & \text{若 } \mathbb{G}^{[\imath-1]}\neq\emptyset,\\ \mathbb{G} & \text{否则}.\end{cases}$$

在两种情形，对任意 $\mathrm{level}(\mathbb{F})\leq j\leq \imath-1$ 和 $\bar{\boldsymbol{x}}_j\in\mathrm{Proj}_{\boldsymbol{x}_j}\mathrm{Zero}(\mathbb{F}/\mathbb{G}^*)$, 由 (4.1.4) 和 (4.1.5), 并注意到 $\mathrm{Zero}(T/\mathbb{G}\cup\{\mathrm{ini}(T)\})=\mathrm{Zero}(T/\mathbb{G})$, 都存在 $\bar{x}_{j+1},\cdots,\bar{x}_\imath\in\tilde{\mathcal{K}}$, 使得

$$\bar{\boldsymbol{x}}_\imath\in\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G}). \tag{4.2.10}$$

对于 (4.2.10), 根据上面的 (A) 存在 $\bar{x}_{i+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\emptyset/\mathbb{U})$. 所以 $\bar{\boldsymbol{x}}\in\mathrm{Zero}([T]/\mathbb{U})$, 因而 (4.2.9) 式成立.

情形 (ii). $\mathbb{T}\neq\emptyset$.

依据归纳原理, 我们假设 (B) 中的性质在执行步骤 T2.2.4 之后对 $i=p$ 成立, 这里 $p=\mathrm{cls}(\mathrm{op}(1,\mathbb{T}))$. 注意, 步骤 T2.2.5 和 T2.2.1 是平凡的, 步骤 T2.2.2 的执行不改变 $\mathbb{T}$ 和 $\mathbb{U}$, 且就这一步而言由 (2.3.5) 知 $[\mathbb{F}^*\cup\{T\},\mathbb{G}^*]$ 的任意零点也是 $[\mathbb{F},\mathbb{G}]$ 的零点. 所以, 我们有下面的 (B′), 它对应于 (B) 在 $j=\mathrm{level}(\mathbb{F})$ 的情形:

(B′) 如果对某个 i 执行步骤 T2.2.2, 那么在执行之后, 对任意 $(\bar{x}_1,\cdots,\bar{x}_i)\in\mathrm{Proj}_{\boldsymbol{x}_i}\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G})$ 有

$$\mathrm{Zero}(\mathbb{T}^{\langle\bar{x},i\rangle}/\mathbb{U}^{\langle\bar{x},i\rangle})\neq\emptyset.$$

(A) 对于步骤 T2.2.3, 我们有

$$\psi=[\mathbb{F},\mathbb{G},\mathbb{T},\mathbb{U}],\quad \psi^*=[\mathbb{F},\mathbb{G}^*,\mathbb{T},\mathbb{U}^*],$$

其中 $\mathbb{U}^*=\mathbb{U}\cup\mathbb{G}^{[i]}$. 对任意 $\bar{\boldsymbol{x}}_i\in\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G}^*)$, 按照 (4.2.2) 存在 $\bar{x}_{i+1},\cdots,\bar{x}_p\in\tilde{\mathcal{K}}$, 使得

$$\bar{\boldsymbol{x}}_p\in\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G}).$$

因此, 由 (B′) 存在 $\bar{x}_{p+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}/\mathbb{U})$. 由于 $\mathbb{U}^{*(p)}=\mathbb{G}^{[i]}\subset\mathbb{G}$, 所以

$$\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}/\mathbb{U}^{*(p)}\cup\mathbb{U})=\mathrm{Zero}(\mathbb{T}/\mathbb{U}^*),$$

于是 (4.2.8) 式成立.

(B) 与情形 (i) 中的 (B) 类似, 对任意 $\mathrm{level}(\mathbb{F})\leq j\leq i-1$ 和 $\bar{\boldsymbol{x}}_j\in\mathrm{Zero}(\mathbb{F}/\mathbb{G}^*)$, 由 (4.1.4) 和 (4.1.5), 并注意到

$$\mathrm{Zero}(T/\mathbb{G}\cup\{\mathrm{ini}(T)\})=\mathrm{Zero}(T/\mathbb{G}),$$

存在 $\bar{x}_{j+1},\cdots,\bar{x}_i\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}_i\in\mathrm{Zero}(\mathbb{F}\cup\{T\}/\mathbb{G})$. 根据上面情形 (ii) 中的 (A), 存在 $\bar{x}_{i+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}/\mathbb{U})$. 所以 $\bar{\boldsymbol{x}}\in\mathrm{Zero}([T]\cup\mathbb{T}/\mathbb{U})$, 因而 (4.2.9) 式也成立. 至此, 断言 (A) 和 (B) 已获得证明.

以下我们证明, 在执行步骤 T2.3 之后, (4.2.8) 式对任意 $\bar{\boldsymbol{x}}_i\in\mathrm{Zero}(\mathbb{F}/\mathbb{G})$ 成立.

若 $\mathbb{T}=\emptyset$, 则步骤 T2.2 的执行是平凡的, 而执行步骤 T2.3 与执行情形 (i) 中 (A) 的步骤 T2.2.3 在 $i=k$ 的情形是一样的; 关于这一点只需注意到多项式 T 在 ProjA 中并不扮演任何特殊角色. 因此, 对任意 $\bar{\boldsymbol{x}}_k\in\mathrm{Zero}(\mathbb{F}/\mathbb{G}^*)$ 都存在 $\bar{x}_{k+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}$ 不是 $\mathbb{U}^*\subset\mathbb{G}$ 中任一多项式的零点. 所以 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\emptyset/\mathbb{U}^*)$, 因而 (4.2.8) 式成立.

如果 $\mathbb{T}\neq\emptyset$, 那么步骤 T2.2.4 必定在之前, 譬如说对 $i=p>k$, 已经执行过, 这里 $p=\mathrm{cls}(\mathrm{op}(1,\mathbb{T}))$. 现在执行步骤 T2.3 与执行情形 (ii) 中 (A) 的步骤 T2.2.3 在 $i=k$ 的情形一样. 因此, 对任意 $\bar{\boldsymbol{x}}_k\in\mathrm{Zero}(\mathbb{F}/\mathbb{G}^*)$ 存在 $\bar{x}_{k+1},\cdots,\bar{x}_n\in\tilde{\mathcal{K}}$, 使得 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{T}/\mathbb{U}^*)$, 于是 (4.2.8) 式也成立.

显而易见, 最终求得的 $[\mathbb{F},\mathbb{G},\mathbb{T},\mathbb{U}]$ 是 TriSerP 说明中的某一个 $\psi_i=[\mathbb{P}_i,\mathbb{Q}_i,\mathbb{T}_i,\mathbb{U}_i]\in\Psi$. 在计算 ψ_i 的过程中, 步骤 T2.2.3 必定对所有 $i\in\{\mathrm{cls}(T):\ T\in\mathbb{T}_i\}$ 都已执行过, 而步骤 T2.3 对 $i=k$ 也已经执行过. 从分裂过程以及原来系统与分裂所得的系统之间保持的零点关系, 我们知道每个 $[\mathbb{P}_i\cup\mathbb{T}_i^{(j)},\mathbb{Q}_i\cup\mathbb{U}_i^{(j)}]$ 都是从某个相应于断言 (A) 中的 $[\mathbb{F}\cup\{T\},\mathbb{G}]$ 在 $i=j$ 的情形产生的, 且使得任意

$$(\bar{x}_1,\cdots,\bar{x}_j)\in\mathrm{Zero}(\mathbb{P}_i\cup\mathbb{T}_i^{(j)}/\mathbb{Q}_i\cup\mathbb{U}_i^{(j)})$$

也是 $[\mathbb{F}\cup\{T\},\mathbb{G}]$ 的零点. 因此, 由 (A) 得

$$\mathrm{Zero}(\mathbb{T}_i^{[j]\langle\bar{x},j\rangle}/\mathbb{U}_i^{[j]\langle\bar{x},j\rangle})\neq\emptyset.$$

换言之, $[\mathbb{T}_i^{[j]\langle\bar{x},j\rangle},\mathbb{U}_i^{[j]\langle\bar{x},j\rangle}]$ 对任意 $j\in\{k\}\cup\{\mathrm{cls}(T):\ T\in\mathbb{T}_i\}$ 都是完美的. 由于

$$\mathrm{Zero}(\mathbb{T}_i^{\langle\bar{x},k\rangle}/\mathbb{U}_i^{\langle\bar{x},k\rangle})\neq\emptyset\Longrightarrow\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)\neq\emptyset,$$

所以依据定义知三角系统 $[\mathbb{T}_i,\mathbb{U}_i]$ 也是完美的.

至此, 算法 TriSerP 的正确性证毕. □

附带指出, 正则和简单系统都具有强投影性质 (见推论 3.2.14 和 3.4.2).

注 4.2.1 可对 TriSerP 中步骤 T2.2.1 的第二个 "若" 条件加以修改以便投影步骤 T2.2.3 在 $\mathrm{level}(\mathbb{F})<i$ 时也执行. 这样一来, 对每个 i, ProjA 都被调用, 而步骤 P2.2.1 中的 V_l 在每次调用时都只含有 x_i. 这一修改能使论述和证明稍加简化. 此时, 可将说明中的性质 (b) 和 (c) 相应地修改如下:

(b′) 对任意 $k\leq j<n$,

$$\mathrm{Proj}_{\boldsymbol{x}_j}=\bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{P}_i\cup\mathbb{T}_i^{(j)}/\mathbb{Q}_i\cup\mathbb{U}^{(j)});$$

(c$'$) 对任意 $1 \le i \le e$ 和

$$k \le j < n, \quad \bar{\boldsymbol{x}}_j \in \mathrm{Zero}(\mathbb{P}_i \cup \mathbb{T}_i^{(j)}/\mathbb{Q}_i \cup \mathbb{U}^{(j)}),$$

$[\mathbb{T}_i^{[j]\langle\bar{x},j\rangle}, \mathbb{U}_i^{[j]\langle\bar{x},j\rangle}]$ 都是完美三角系统，因而 $[\mathbb{T}_i^{[j]}, \mathbb{U}_i^{[j]}]$ 也是.

如果 $k = 0$, 那么每个 $[\mathbb{T}_i, \mathbb{U}_i]$ 都具有强投影性质. 可是，如果分裂在 $\mathrm{level}(\mathbb{F}) < \imath \neq k$ 时也发生，则上述修改有一个关键性的弊端：在步骤 T2.2.2 中对同样的 $\mathbb{F}$, Elim 会被重复调用.

注 4.2.2 可用一个更为复杂的程序对投影步骤 T2.2.4 作如下修改：现不再计算

$$\mathrm{prem}\left(\prod_{G\in\mathbb{G}^{[\imath-1]}} G^{\mathrm{ldeg}(T)}, T\right),$$

而是在将 T 变为无平方因子之后计算 T 和每个多项式 $G \in \mathbb{G}^{[\imath-1]}$ 关于 $x_\imath$ 的最大公因子，譬如用伪除法，并将该公因子从 T 和 G 中抹去. 在抹去所有这样的公因子之后，T 与 $\mathbb{G}^{[\imath-1]}$ 中每个多项式的最大公因子都应为 1. 因此，$\mathrm{Zero}(T/\mathbb{G}^{[\imath-1]}) \neq \emptyset$ 当且仅当 T 关于 $x_\imath$ 的次数是正的 (见 [63]). 在计算最大公因子的同时，所考虑的系统被分裂为有限多个其他系统以便保持必要的零点关系. 这一技术已在算法 SimSer 中反映出来. 事实上，从 SimSer 可以导出另一投影算法.

算法 TriSerP 对代数闭域的存在性理论提供了一个量词消去程序 —— 因而一个判定程序. 作为该算法的推论，我们有下面的投影定理.

定理 4.2.1 (消去理论的投影定理 —— 仿射情形) 设 $\{\mathbb{F}_i(\boldsymbol{x}, \boldsymbol{y}) : 1 \le i \le s\}$ 为一组 $\mathcal{K}$ 上以

$$\boldsymbol{x} = (x_1, \cdots, x_n), \quad \boldsymbol{y} = (y_1, \cdots, y_m)$$

为变元的多项式方程和不等方程的有限合取，那么存在有限多个 $\mathbb{G}_j(\boldsymbol{x})$, 其中每个都是 $\mathcal{K}$ 上具有下述性质的多项式方程和不等方程的有限合取：对 $\mathcal{K}$ 的某一扩域 $\tilde{\mathcal{K}}$ 上的仿射空间 $\mathbf{V}^n$ 中的每一点 $\bar{\boldsymbol{x}} = (\bar{x}_1, \cdots, \bar{x}_n)$, 都存在 $\tilde{\mathcal{K}}$ 的某一代数扩域上的仿射空间 $\mathbf{W}^m$ 中的一点 $\bar{\boldsymbol{y}} = (\bar{y}_1, \cdots, \bar{y}_m)$, 使得 $(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}})$ 至少满足 $\mathbb{F}_i(\boldsymbol{x}, \boldsymbol{y})$ 中之一当且仅当 $\bar{\boldsymbol{x}}$ 满足 $\mathbb{G}_j(\boldsymbol{x})$ 中之一.

该定理的证明之一已在塔斯基的经典判定方法中出现并由雅各布森在 [33] 中 (5.4 节 305 和 306 页) 予以阐明. 另一证明见诸于 [63, 64], 而最近的一个证明则由吴文俊给出 [103].

对 (4.2.4) 中的每个多项式系统 $[\mathbb{P}_i, \mathbb{Q}_i]$, 我们可以用算法 CharSer, TriSer 或 TriSerS 来进一步计算它的三角序列. 相应的零点分解可与 (4.2.4) 合在一起. 作为推论, 即有一算法, 它可对任意多项式系统 $[\mathbb{P}, \mathbb{Q}]$ 和整数 $0 \le k < n$ 计算集合 Ψ, 该集合或者是空的, 因而 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$, 或者具有如下形式:

$$\{[\mathbb{P}_1, \mathbb{Q}_1, \mathbb{T}_1, \mathbb{U}_1], \cdots, [\mathbb{P}_e, \mathbb{Q}_e, \mathbb{T}_e, \mathbb{U}_e]\},$$

使得 TriSerP 说明中的 (a), (b) 和 (c) 都成立, 并且每个 $[\mathbb{P}_i \cup \mathbb{T}_i, \mathbb{Q}_i \cup \mathbb{U}_i]$ 都是具有 k 维投影性质的 (良好) 三角系统, 其中 $\mathbb{P}_i$ 排为三角列. 这时, 我们称 $n-k$ 为投影的 **维数**. 若投影的维数是 n, 则说消元是带有 **全** 投影的; 若维数是 0, 则说消元是 **不带** 投影的.

例 4.2.2 考虑例 3.1.2 中给出的多项式组 $\mathbb{P}$ 与变元序 $x \prec y \prec u \prec v \prec w$. 用 TriSerP 对 w, v, u 带投影可将 $\mathbb{P}$ 分解为五个良好三角系统 $\mathfrak{T}_i = [\mathbb{T}_i, \mathbb{U}_i]$, 使得零点分解 (2.1.7) 对 $\mathbb{Q} = \emptyset$ 及 $e = 5$ 成立, 且每个 $\mathfrak{T}_i$ 都具有 2 维 (强) 投影性质. 下面列出的三角列 $\mathbb{T}_i$ 以及相应的 $\mathbb{U}_i$ 将在例 9.2.2 中用到.

$$\begin{aligned}
\mathbb{T}_1 &= [T_{11}, T_{12}, P_3, P_4],\\
\mathbb{T}_2 &= [T_{21}, T_{22}, F, P_3, P_4],\\
\mathbb{T}_3 &= [T_{31}, G, T_{33}, P_3, P_4],\\
\mathbb{T}_4 &= [T_{41}, y, 12\,xu + 2\,u - 9\,x^2 - 2\,x + 9, v^2 + u^2 - 2\,xu + x^2 - 1, P_4],\\
\mathbb{T}_5 &= [x, 729\,y^4 - 956\,y^2 - 529, u\,(85\,u - 81\,y^2 + 72), u\,(3\,uv + 2\,v - 3\,uy), P_4],
\end{aligned}$$

其中

$$\begin{aligned}
T_{21} &= 243\,x^2 + 36\,x + 85,\\
T_{22} &= 10460353203\,y^6 - 6377292\,(8523\,x + 4535)\,y^4\\
&\quad + 648\,(155380149\,x + 61648)\,y^2 - 16\,(2250218592\,x - 1609630283),
\end{aligned}$$

$T_{11}, T_{12}, F, T_{31}, G, T_{33}, T_{41}$ 与例 3.1.2 中相同, 而

$$\begin{aligned}
\mathbb{U}_1 = \{&x, y, T_{21}, \mathrm{ini}(T_{12}), T_{32},\\
&729\,(2187\,x^6 - 1134\,x^5 - 7326\,x^4 + 4144\,x^3 + 2015\,x^2 - 6498\,x\\
&- 2268)\,y^4 - 2\,(1594323\,x^9 + 2007666\,x^8 + 2591595\,x^7\\
&+ 6800112\,x^6 - 12642075\,x^5 + 2179818\,x^4 + 4872429\,x^3
\end{aligned}$$

$$
\begin{aligned}
& - 12546172\,x^2 - 7821216\,x - 1084104)\,y^2 + 1594323\,x^{12} \\
& + 590490\,x^{11} - 12328119\,x^{10} - 6466230\,x^9 + 22602402\,x^8 \\
& + 8733636\,x^7 - 22926870\,x^6 + 11418356\,x^5 + 35613711\,x^4 \\
& + 1579842\,x^3 - 13321235\,x^2 - 318366\,x + 1199772\}, \\
\mathbb{U}_2 &= \{x, y, 4194\,x - 935, -6561\,y^2 + 16344\,x + 4132, 1162261467\,xy^4 \\
& - 26244\,(35676\,x - 79985)\,y^2 - 40\,(61438590\,x + 29843347)\}, \\
\mathbb{U}_3 &= \{x, y, T_{21}, 8474827586184\,x^5 - 6240413571255\,x^4 \\
& + 7521969157884\,x^3 + 2321430215166\,x^2 + 3035377934972\,x \\
& + 1281758320845, 18\,x - 1, U\}, \\
\mathbb{U}_4 &= \{9\,x^2 + 2\,x - 9, 6\,x + 1, x^3 + 54\,x^2 + 27\,x - 52\}, \\
\mathbb{U}_5 &= \{y, 5653\,y^2 - 2116, U\}.
\end{aligned}
$$

$\mathbb{U}_3$ 和 $\mathbb{U}_5$ 中的多项式 U 由于过大而未在这里给出. 它是不可约的, 有 91 项, 关于 x, y, u 的次数分别为 15, 10, 1.

投影的应用包括参数代数系统求解, 轨迹方程的自动推导, 参数对象的隐式化和确定奇点的存在性条件. 这些应用将在 7.4 和 9.1–9.3 节中予以讨论.

4.3 三角列的不可约性

定义 4.3.1 三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 称为是*拟不可约的*, 如果 $\mathbb{T}$ 中每个多项式在基域 $\mathcal{K}$ 上都是不可约的.

$\mathcal{K}[\boldsymbol{x}]$ 中的三角系统 $[\mathbb{T}, \mathbb{U}]$ 称为是*拟不可约的*, 如果 $\mathbb{T}$ 是拟不可约的.

用 $\mathcal{K}$ 上的多项式因子分解, 不难计算出形如 (2.2.6) 和 (2.1.7) 的零点分解使得其中所有三角列都是拟不可约的. 这可以通过因子分解将多项式系统分裂而得以实现. 更具体地说, 对任意多项式系统 $[\mathbb{P}, \mathbb{Q}]$, 如果 $P_1, \cdots, P_t$ 是某个多项式 $P \in \mathbb{P}$ 的所有不可约因子, 则有

$$
\operatorname{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{j=1}^{t} \operatorname{Zero}(\mathbb{P}_j/\mathbb{Q}), \tag{4.3.1}
$$

其中

$$
\mathbb{P}_j = \mathbb{P} \setminus \{P\} \cup \{P_j\}, \quad 1 \le j \le t.
$$

作为 4.4 节中介绍的 IrrTriSer 的子算法, 我们对算法 TriSer 作适当修改以得到如下的 QuaIrrTriSer.

算法 QuaIrrTriSer: $\Psi \leftarrow \text{QuaIrrTriSer}(\mathbb{P},\mathbb{Q},\mathbb{T})$. 给定三元组 $[\mathbb{P},\mathbb{Q},\mathbb{T}]$, 其中 $[\mathbb{T},\mathbb{Q}]$ 构成拟不可约三角系统而 $\mathbb{Q}$ 中所有多项式对 $\mathbb{T}$ 都是约化的, 本算法计算良好拟不可约三角系统 $[\mathbb{T}_1,\mathbb{U}_1],\cdots,[\mathbb{T}_e,\mathbb{U}_e]$ 组成的有限集合 Ψ, 使得

$$\text{Zero}(\mathbb{P}\cup\mathbb{T}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\mathbb{U}_i). \tag{4.3.2}$$

和前面一样, 在 $\text{Zero}(\mathbb{P}\cup\mathbb{T}/\mathbb{Q}) = \emptyset$ 得以验证时 $\Psi=\emptyset$. 在 $\mathbb{T}=\emptyset$ 的情形, QuaIrrTriSer 将任意多项式系统 $[\mathbb{P},\mathbb{Q}]$ 分解为良好的拟不可约三角系统. 算法 QuaIrrTriSer 是从 TriSer 通过用

T1′. 命 $\Psi \leftarrow \emptyset$, $\Phi \leftarrow \{[\mathbb{P},\mathbb{Q},\mathbb{T}]\}$.

替换 **T1**, 且用

P2.3′. 计算 T 在 $\mathcal{K}$ 上的所有不可约因子 $F_1,\cdots,F_t$, 且命 $\bar{\mathbb{G}} \leftarrow \mathbb{G}$.

P2.3″. 对 $j=1,\cdots,t$ 执行下列步骤:

P2.3.1. 计算 $\bar{\mathbb{G}}' \leftarrow \text{prem}(\bar{\mathbb{G}},F_j)$.

P2.3.2. 若 $j=1$, 则命 $\mathbb{G} \leftarrow \bar{\mathbb{G}}'$, $T \leftarrow F_j$. 否则的话, 若 $0 \notin \bar{\mathbb{G}}'$, 则命 $\Omega \leftarrow \Omega \cup \{[\mathbb{F},\bar{\mathbb{G}}',[F_j]\cup\mathbb{T}]\}$.

替换 PriTriSys 中的 **P2.3** 而获得.

证 关于步骤 T1 到 T1′ 的修改, 这里的 $\mathbb{P}\cup\mathbb{T}$ 对应于 TriSer 的输入集合 $\mathbb{P}$, 而 $\mathbb{T}$ 中多项式的初式可能为零的情形不必考虑, 原因是 $[\mathbb{T},\mathbb{Q}]$ 为三角系统. 实际上, 算法 TriSer 中 Φ 中的任意三元组都与 QuaIrrTriSer 的输入三元组具有相同的形式. 关于步骤 P2.3 到 P2.3′ 和 P2.3″ 的修改, 由 Elim 生成的多项式 T 在基域 $\mathcal{K}$ 上分解为不可约因子, 相应的多项式系统则通过用 T 的因子来替换 T 而分裂为子系统. 不难看出, 对在步骤 P2.3.2 中生成的任意三元组, 譬如说 $[\mathbb{F}^*,\mathbb{G}^*,\mathbb{T}^*]$, 都有 $\text{level}(\mathbb{F}^*) < \text{level}(\mathbb{F})$, 其中 $\mathbb{F}$ 是从步骤 T2.1 的 Φ 中选取的相应三元组之第一个分量 (参见 TriSer 的终止性证明). 所以, 算法 QuaIrrTriSer 同样终止.

关于该算法的正确性, 我们只需注意到通过因子分解分裂多项式系统的零点关系 (4.3.1). 对于关系式 (4.3.2) 的证明, 可采用证明算法 TriSer 中 (2.1.7) 式所用到的同样论据. 由于相应的 T 已被其不可约因子所替代, 根据定义 $\mathbb{T}_i$ 是拟不可约的, 因此 $[\mathbb{T}_i,\mathbb{U}_i]$ 对每个 i 也都是如此. 又因为 $\mathbb{U}_i$ 中的所有多项式实际上都是某些多项式对 $\mathbb{T}_i$ 的伪余式 (因而对 $\mathbb{T}_i$ 也是约化的), 所以 $[\mathbb{T}_i,\mathbb{U}_i]$ 是良好的. □

顺便提及，类 $< i$ 的那些 F_j 都是 T 的初式的因子，因而不必考虑．所以相应的三元组都可从集合 Ω 中删去．

例 4.3.1 重温例 2.3.1 和 2.3.2，并将算法 QualrrTriSer 用到级为 4 的三元组 $[\mathbb{P},\emptyset,\emptyset]$．容易验证，算法 TriSer 求得的三角列 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 中的所有多项式都是不可约的．然而 $\mathbb{T}_3$ 中的第一个多项式 t^3+1 是可约的，并可分解为两个多项式

$$t-1,\ \ T_1=t^2+t+1$$

的乘积．所以，在 QualrrTriSer 中 $[\mathbb{T}_3,\mathbb{U}_3]$ 分裂为两个三角系统 $[\mathbb{T}_3',\mathbb{U}_3']$ 和 $[\mathbb{T}_3'',\mathbb{U}_3'']$，其中

$$\begin{aligned}
\mathbb{T}_3' &= [T_1,-z^5+t^4,-z^3y-t^3,zx^2-t],\\
\mathbb{T}_3'' &= [t-1,-z^5+t^4,-z^3y-t^3,zx^2-t],\\
\mathbb{U}_3' &= \mathbb{U}_3''=\{z\}.
\end{aligned}$$

将三角列 $\mathbb{T}$ 写成 (2.1.1) 的形式，并将导元 $x_{p_1},\cdots,x_{p_r}$ 重新命名为 $y_1,\cdots,y_r$．又将所有其他变元记作 $u_1,\cdots,u_d$ 或 $\boldsymbol{u}$，那么 $\mathbb{T}$ 可以写为

$$\mathbb{T}=\begin{bmatrix} T_1(\boldsymbol{u},y_1), \\ T_2(\boldsymbol{u},y_1,y_2), \\ \cdots\cdots\cdots\cdots \\ T_r(\boldsymbol{u},y_1,y_2,\cdots,y_r) \end{bmatrix}. \tag{4.3.3}$$

设 $\mathcal{K}_0$ 为 $\mathcal{K}$ 通过添加 $u_1,\cdots,u_d$ 所得的超越扩域 $\mathcal{K}(\boldsymbol{u})=\mathcal{K}(u_1,\cdots,u_d)$．我们归纳定义 $\mathbb{T}$ 的 *不可约性* 和 *一般零点* 如下．

定义 4.3.2 只含一个多项式 $T_1(\boldsymbol{u},y_1)$ 的良好三角列 $\mathbb{T}$ 称为是 *不可约的*，如果 T_1 作为 $\mathcal{K}_0[y_1]$ 中的多项式是不可约的．此时，设 η_1 为 T_1 在 $\mathcal{K}_0$ 的某一代数扩域中的零点，则称 $(\boldsymbol{u},\eta_1)$ 为 $\mathbb{T}$ 的一个 *一般零点*．

现假设任意长度 $< r$ 的良好三角列之不可约性和一般零点的定义都已给出．

如 (4.3.3) 所示的长度 $r>1$ 的良好三角列 $\mathbb{T}$ 称为是 *不可约的*，如果良好三角列

$$\mathbb{T}^{\{r-1\}}=[T_1,\cdots,T_{r-1}]$$

是不可约的，以 $(\boldsymbol{u},\eta_1,\cdots,\eta_{r-1})$ 为一般零点，而且多项式

$$\bar{T}_r=T_r(\boldsymbol{u},\eta_1,\cdots,\eta_{r-1},y_r)\in\mathcal{K}_{r-1}[y_r]$$

在 $\mathcal{K}_{r-1}$ 上不可约，这里 $\mathcal{K}_{r-1}=\mathcal{K}_0(\eta_1,\cdots,\eta_{r-1})$ 是通过将 $\eta_1,\cdots,\eta_{r-1}$ 添入 $\mathcal{K}_0$ 所得的代数扩域. 此时，设 η_r 为 $\bar{T}_r$ 在 $\mathcal{K}_{r-1}$ 的某一代数扩域中的零点，则称 $(\boldsymbol{u},\eta_1,\cdots,\eta_r)$ 为 $\mathbb{T}$ 的一个 *一般零点*.

良好三角系统 $[\mathbb{T},\mathbb{U}]$ 称为是 *不可约的*, 如果 $\mathbb{T}$ 是不可约的.

设 $\mathbb{T}$ —— 如 (4.3.3) 所示 —— 是一个以 $(\boldsymbol{u},\eta_1,\cdots,\eta_r)$ 为一般零点的不可约三角列. 为简略起见，我们有时将 $(\boldsymbol{u},\eta_1,\cdots,\eta_i)$ 写成 $\boldsymbol{\xi}_i$, 且令 $\boldsymbol{\xi}=\boldsymbol{\xi}_r$. 又称 $T_1,\cdots,T_r$ 为扩域 $\mathcal{K}_r=\mathcal{K}(\boldsymbol{\xi})$ 的 *添加多项式*, $\mathbb{T}$ 为 $\mathcal{K}_r$ 的 *添加三角列*. 很明显，$\mathbb{T}$ 的每个一般零点 $\boldsymbol{\xi}$ 都可视为线性空间 $\tilde{\mathcal{K}}^n$ 中的一个点. 上面的 $d=|\boldsymbol{u}|$, 即参数的个数，称为 $\mathbb{T}$ 的 *维数*, 记作 $\dim(\mathbb{T})$.

如果上述良好三角列 $\mathbb{T}$ 是可约的，则存在 k, 使得 $\mathbb{T}^{\{k-1\}}$ 不可约且以

$$\boldsymbol{\xi}_{k-1}=(\boldsymbol{u},\eta_1,\cdots,\eta_{k-1})$$

为一般零点，而多项式

$$\bar{T}_k=T_k(\boldsymbol{\xi}_{k-1},y_k)\in\mathcal{K}_{k-1}[y_k]$$

在 $\mathcal{K}_{k-1}=\mathcal{K}(\boldsymbol{\xi}_{k-1})$ 上是可约的. 设 $\mathcal{K}_{k-1}[y_k]$ 中的 $\bar{T}_k$ 有一不可约因子分解

$$\bar{T}_k=H_1\cdots H_t,$$

其中每个 $H_i\in\mathcal{K}_{k-1}[y_k]$ 在 $\mathcal{K}_{k-1}$ 上都是不可约的, 而 $t\geq 2$. 系数 $\mathrm{coef}(H_i,y_k^j)$ 都是 $\mathcal{K}_{k-1}$ 中的元素，因此可以表示为 $\boldsymbol{\xi}_{k-1}$ 的多项式的商. 于是经通分可得表达式

$$\bar{D}\bar{T}_k=\bar{F}_1\cdots\bar{F}_t,$$

这里

$$\begin{aligned}&D\in\mathcal{K}[\boldsymbol{u},y_1,\cdots,y_{k-1}],\quad F_i\in\mathcal{K}[\boldsymbol{u},y_1,\cdots,y_k],\\&\bar{D}=D(\boldsymbol{\xi}_{k-1})\in\mathcal{K}_{k-1},\quad \bar{F}_i=F_i(\boldsymbol{\xi}_{k-1},y_k)\in\mathcal{K}_{k-1}[y_k].\end{aligned}$$

可假定多项式 D 对 $\mathbb{T}^{\{k-1\}}$ 是约化的, 也可假定每个 F_i 对 $\mathbb{T}^{\{k\}}$ 都是约化的.

视 y_k 为自由变元，并将其更名为 v, 那么

$$\boldsymbol{\xi}^{*\{k-1\}}=(v,\boldsymbol{u},\eta_1,\cdots,\eta_{k-1})$$

是 $\mathbb{T}^{\{k-1\}}\subset\mathcal{K}[v,\boldsymbol{u},y_1,\cdots,y_{k-1}]$ 的一个一般零点. 令

$$G=F_1\cdots F_t-DT_k\in\mathcal{K}[v,\boldsymbol{u},y_1,\cdots,y_{k-1}].$$

由于 $\bar{D}\bar{T}_k = \bar{F}_1 \cdots \bar{F}_t$, 我们有 $G(\boldsymbol{\xi}^{*\{k-1\}}) = 0$. 故由引理 4.5.1 得

$$\mathrm{prem}(G, \mathbb{T}^{\{k-1\}}) = 0.$$

因此存在非负整数 $s_1, \cdots, s_{k-1}$ 和多项式 $Q_1, \cdots, Q_{k-1} \in \mathcal{K}[v, \boldsymbol{u}, y_1, \cdots, y_{k-1}]$, 使得

$$I_1^{s_1} \cdots I_{k-1}^{s_{k-1}} G = I_1^{s_1} \cdots I_{k-1}^{s_{k-1}} (F_1 \cdots F_t - DT_k) = \sum_{i=1}^{k-1} Q_i T_i,$$

或

$$I_1^{s_1} \cdots I_{k-1}^{s_{k-1}} F_1 \cdots F_t = \sum_{i=1}^{k} Q_i T_i. \tag{4.3.4}$$

上面将 y_k 更名的目的是为了帮助理解引理 4.5.1 的应用, 它并没有什么实际影响. 诸 Q_i 都是变元 $\boldsymbol{u}, y_1, \cdots, y_k$ 的多项式.

我们将以上讨论总结为下面的引理.

引理 4.3.1 有一算法, 它能

(a) 判定良好三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{u}, \boldsymbol{y}]$ 是否不可约;

若 $\mathbb{T}$ 可约:

(b) 确定整数 k, 使得由 $\mathbb{T}$ 的前 $k-1$ 项构成的三角列 $\mathbb{T}^{\{k-1\}}$ 不可约, 且以 $\boldsymbol{\xi}_{k-1}$ 为一般零点, 而多项式 $T_k(\boldsymbol{\xi}_{k-1}, y_k)$ 在 $\mathcal{K}_{k-1} = \mathcal{K}(\boldsymbol{\xi}_{k-1})$ 上是可约的;

(c) 求得 T_k 在 $\mathcal{K}_{k-1}$ 上的不可约因子分解

$$DT_k \doteq F_1 \cdots F_t, \tag{4.3.5}$$

这里多项式

$$D \in \mathcal{K}[\boldsymbol{u}, y_1, \cdots, y_{k-1}], \quad F_i \in \mathcal{K}[\boldsymbol{u}, y_1, \cdots, y_k], \ 1 \le i \le t,$$

对 $\mathbb{T}^{\{k-1\}}$ 都是约化的, 而带点的等式意指 $\mathrm{prem}(DT_k - F_1 \cdots F_t, \mathbb{T}^{\{k-1\}}) = 0$.

现将引理 4.3.1 所指明的算法述之如下.

算法 Factor: $[k, D, \mathbb{F}] \leftarrow \mathrm{Factor}(\mathbb{T})$. 任给良好三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算整数 k, 多项式 D 和 $\mathcal{K}[\boldsymbol{x}]$ 中多项式组成的有限集合 $\mathbb{F}$, 使得 $0 \le k \le |\mathbb{T}|$, 并且

(a) 若 $k=0$, 则 $\mathbb{T}$ 不可约;

(b) 若 $k=1$, 则 $\mathbb{T}$ 是可约的, $|\mathbb{F}|>1$, $\mathbb{T}$ 中的第一个、类为 p_1 的多项式 T_1 在 $\mathcal{K}_0=\mathcal{K}(x_1,\cdots,x_{p_1-1})$ 上具有因子分解 $T_1=\prod_{F\in\mathbb{F}}F$, 且每个 $F\in\mathbb{F}\subset\mathcal{K}_0[x_{p_1}]$ 在 $\mathcal{K}_0$ 上都是不可约的;

(c) 若 $k>1$, 则 $\mathbb{T}$ 是可约的, $\mathbb{T}^{\{k-1\}}$ 是不可约的, $|\mathbb{F}|>1$, $\mathbb{T}$ 中的第 k 个多项式 T_k 在 $\mathcal{K}$ 的以 $\mathbb{T}^{\{k-1\}}$ 为添加三角列的扩域 $\mathcal{K}_{k-1}$ 上具有因子分解 $DT_k\doteq\prod_{F\in\mathbb{F}}F$, 且每个 $F\in\mathbb{F}\subset\mathcal{K}_{k-1}[x_{p_k}]$ 在 $\mathcal{K}_{k-1}$ 上都是不可约的.

在上面的说明 (c) 中, 从 $\mathcal{K}$ 得到扩域 $\mathcal{K}_{k-1}$ 的方式稍有不同:

$$\mathcal{K}_{k-1}=\mathcal{K}(x_1,\cdots,x_{p_k-1}),$$

这里 $x_{p_j}=\mathrm{lv}(T_j)$ 看作以 T_j 为添加多项式的代数元, $1\le j\le k-1$, 而其他 x_i 则是添加的超越元. 我们将代数扩域上的多项式因子分解简称为 *代数因子分解*, 并在 9.4 节中简略介绍两个代数因子分解算法.

4.4 分解为不可约三角系统

从公式 (4.3.4) 容易建立下面的分解引理.

引理 4.4.1 设多项式组 $\mathbb{P}$ 有中间列 $\mathbb{T}=[T_1,\cdots,T_r]$, 这里

$$\mathrm{cls}(T_1)>0,\quad I_i=\mathrm{ini}(T_i),\quad 1\le i\le r.$$

假定 $\mathbb{T}$ 可约, 因此存在 k, 使得 T_k 能分解为不可约多项式 $F_1,\cdots,F_t$ 而得到形如 (4.3.5) 的不可约因子分解, 那么下面的零点分解成立:

$$\mathrm{Zero}(\mathbb{P})=\bigcup_{i=1}^{k-1}\mathrm{Zero}(\mathbb{P}_i)\cup\bigcup_{j=1}^{t}\mathrm{Zero}(\mathbb{Q}_j),\tag{4.4.1}$$

其中 $\mathbb{P}_i=\mathbb{P}\cup\{I_i\}$ $(1\le i\le k-1)$, 而 $\mathbb{Q}_j=\mathbb{P}\cup\{F_j\}$ $(1\le j\le t)$.

证 $\mathbb{P}_i$ 或 $\mathbb{Q}_j$ 的任意零点都明显是 $\mathbb{P}$ 的零点. 相反, $\mathbb{P}$ 的每个零点都是 T_i 的零点. 由 (4.3.4), 该零点也是某个 I_i 或 F_j 的零点, 因而也是某个 $\mathbb{P}_i$ 或 $\mathbb{Q}_j$ 的零点. □

在引理 4.4.1 中，每个 I_i 对 $\mathbb{T}$ 都已约化，而每个 F_j 又被假定对 $\mathbb{T}^{\{k\}}$ 是约化的，因此对 $\mathbb{T}$ 也是约化的. 所以，由引理 2.2.4, 多项式组 $\mathbb{P}_i \cup \mathbb{C}$ 或 $\mathbb{Q}_j \cup \mathbb{C}$ 的任意中间列都比 $\mathbb{T}$ 有较低的秩. 因而，视每个 $\mathbb{P}_i \cup \mathbb{C}$ 或 $\mathbb{Q}_j \cup \mathbb{C}$ 为 $\mathbb{P}$ 进一步求得形如 (4.4.1) 的零点分解，我们最终将获得与 (2.2.6) 形式一样的分解，而其中的所有 $\mathbb{C}_i$ 都不可约.

特征或三角序列 Ψ 称为是 *不可约的*, 如果 Ψ 中的每个升列或三角系统都是不可约的. 下面的算法指出如何从任给多项式组 $\mathbb{P}$ 构造出一个不可约特征序列.

算法 IrrCharSer: $\Psi \leftarrow \text{IrrCharSer}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算 $\mathbb{P}$ 的不可约特征序列 Ψ.

I1. 命 $\Phi \leftarrow \{\mathbb{P}\}$, $\Psi \leftarrow \emptyset$.

I2. 重复下列步骤直至 $\Phi = \emptyset$:

I2.1. 设 $\mathbb{F}$ 为 Φ 中的元素，且命 $\Phi \leftarrow \Phi \setminus \{\mathbb{F}\}$.

I2.2. 计算 $\mathbb{C} \leftarrow \text{CharSet}(\mathbb{F})$.

I2.3. 若 $\mathbb{C}$ 为非矛盾列，则:

I2.3.1 计算 $[k, D, \mathbb{G}] \leftarrow \text{Factor}(\mathbb{C})$.

I2.3.2 若 $k = 0$, 则命

$$\Psi \leftarrow \Psi \cup \{\mathbb{C}\}, \quad \Phi \leftarrow \Phi \cup \{\mathbb{F} \cup \mathbb{C} \cup \{I\} \colon I \in \text{ini}(\mathbb{C}) \setminus \mathcal{K}\};$$

否则，命

$$\begin{aligned}\Phi \leftarrow \Phi \cup \{\mathbb{F} \cup \mathbb{C} \cup \{I\} \colon I \in \text{ini}(\mathbb{C}^{\{k-1\}}) \setminus \mathcal{K}\} \\ \cup \{\mathbb{F} \cup \mathbb{C} \cup \{G\} \colon G \in \mathbb{G}\}.\end{aligned}$$

例 4.4.1 参见例 2.2.3. 容易验证，那里的特征列 $\mathbb{C}$ 中的第一个多项式 C_1 在 $\mathrm{Q}(x_1)$ 上是不可约的. 为了判定 $\mathbb{C}$ 是否不可约，我们需要知道 $\mathbb{C}$ 中的第二个多项式 C_2 在扩域 $\mathrm{Q}(x_1, \eta)$ 上是否不可约，这里 η 是 C_1 的扩充零点. 应用代数因子分解方法可以确认

$$C_2 \doteq (x_1 + 1)\,(x_3 - 2\,x_1 x_2 + x_1)\,(x_3 + x_1 x_2 - x_1)$$

在 $\mathrm{Q}(x_1, \eta)$ 上成立. 命

$$\begin{aligned}\mathbb{P}_1 &= \mathbb{P} \cup \{x_1\}, & \mathbb{P}_3 &= \mathbb{P} \cup \{x_3 - 2\,x_1 x_2 + x_1\}, \\ \mathbb{P}_2 &= \mathbb{P} \cup \{x_1 + 1\}, & \mathbb{P}_4 &= \mathbb{P} \cup \{x_3 + x_1 x_2 - x_1\}.\end{aligned}$$

根据引理 4.4.1, 我们有以下分解

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{4} \mathrm{Zero}(\mathbb{P}_i).$$

$\mathbb{P}_1 \cup \mathbb{C}$ 和 $\mathbb{P}_2 \cup \mathbb{C}$ 的特征列 $\mathbb{C}_1$ 和 $\mathbb{C}_2$ 已在例 2.2.4 中给出. $\mathbb{P}_3 \cup \mathbb{C}$ 和 $\mathbb{P}_4 \cup \mathbb{C}$ 的特征列分别为

$$\begin{aligned}
\mathbb{C}_3 &= [C_1, x_3 - 2\,x_1x_2 + x_1, x_1\,(x_4 + x_2 - 1)],\\
\mathbb{C}_4 &= [C_1, x_3 + x_1x_2 - x_1, x_1\,(x_4 - 2\,x_2 + 1)].
\end{aligned}$$

C_1 以及 $\mathbb{C}_3$ 和 $\mathbb{C}_4$ 中的第三个多项式的因子 x_1 可以随意抹去; 抹去该因子之后所得的升列仍用 $\mathbb{C}_3$ 和 $\mathbb{C}_4$ 来记.

让我们来检查一下四个升列 $\mathbb{C}_1, \cdots, \mathbb{C}_4$ 是否不可约; $\mathbb{C}_3$ 和 $\mathbb{C}_4$ 二者的确如此, 因为除 C_1 外它们中的所有多项式关于其导元都是线性的. 我们不难发现 $\mathbb{C}_1$ 中的第三个多项式可分解为

$$x_3^2 - 1 = (x_3 - 1)\,(x_3 + 1),$$

而 $\mathbb{C}_2$ 中的第四个多项式在代数扩域 $\mathrm{Q}(x_2)$ 上可分解为

$$x_4^2 - x_2x_4 + 3\,x_2 = (x_4 + x_2 - 1)\,(x_4 - 2\,x_2 + 1),$$

这里 x_2 的添加多项式为 $2\,x_2^2 + 1$. 再用引理 4.4.1, 我们得到进一步的分解, 其中相应的不可约升列如下:

$$\begin{aligned}
\mathbb{C}_1' &= [x_1 + 1, x_2, x_3 + 1, x_4 + 1],\\
\mathbb{C}_1'' &= [x_1 + 1, x_2, x_3 - 1, x_4 - 1],\\
\mathbb{C}_2' &= [x_1, 2\,x_2^2 + 1, x_3, x_4 + x_2 - 1],\\
\mathbb{C}_2'' &= [x_1, 2\,x_2^2 + 1, x_3, x_4 - 2\,x_2 + 1].
\end{aligned}$$

因此, 我们获得 $\mathbb{P}$ 的一不可约特征序列 $\{\mathbb{C}_1', \mathbb{C}_1'', \mathbb{C}_2', \mathbb{C}_2'', \mathbb{C}_3, \mathbb{C}_4\}$ 及相应的零点分解

$$\begin{aligned}
\mathrm{Zero}(\mathbb{P}) = {} & \mathrm{Zero}(\mathbb{C}_1') \cup \mathrm{Zero}(\mathbb{C}_1'') \cup \mathrm{Zero}(\mathbb{C}_2')\\
& \cup \mathrm{Zero}(\mathbb{C}_2'') \cup \mathrm{Zero}(\mathbb{C}_3/x_1 + 1) \cup \mathrm{Zero}(\mathbb{C}_4/x_1 + 1).
\end{aligned}$$

注 4.4.1 同样可以定义不可约弱升列, 但无法定义不可约拟升列. 通过修改相应的概念, 算法 IrrCharSer 也可用来计算多项式组的不可约弱特征序列.

注 4.4.2 除第一个多项式外其他所有多项式关于其导元都是线性的三角列称为是 *拟线性的*. 多项式组的特征列经常是拟线性的. 这一点从特征列算法以伪除为其主要运算这一特色可以看出. 令 $R = \mathrm{prem}(G, F, x)$, 通常有 $\deg(R, x) = \deg(F, x) - 1$, 即被除多项式 G 化为次数比除式 F 的次数小 1 的伪余式 R. 拟线性性的频繁出现使得我们可以声称, 对于计算不可约特征序列, 在正规情形对第一个特征列代数因子分解是不必要的. 这就给 "为什么不可约分解是实际可行的" 作了一个解释. 注意, 一般来说第一个特征列就大小而言是最复杂的. 不幸的是, 在计算特征序列的过程中, 初式的添加经常毁坏了扩大后的多项式组之特征列的拟线性性. 所以, 为了确定这些特征列的不可约性, 代数因子分解又是经常需要的.

引理 4.4.2 设 $[\mathbb{T}, \mathbb{U}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的良好三角系统. 假定 $\mathbb{T}$ 是可约的, 因此存在 k, 使得 $\mathbb{T}$ 的第 k 项 T_k 分解为不可约多项式 $F_1, \cdots, F_t$ 的乘积如 (4.3.5) 所示, 那么下面的零点分解成立:

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{t} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U} \cup \{D\}) \cup \mathrm{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U}), \tag{4.4.2}$$

其中 $\mathbb{T}_i = \mathbb{T} \setminus \{T_k\} \cup \{F_i\}$, $1 \leq i \leq t$.

证 对任意 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}/\mathbb{U})$, 我们有 $T_k(\bar{\boldsymbol{x}}) = 0$, 于是必定存在 i, 使得 $F_i(\bar{\boldsymbol{x}}) = 0$. 若 $D(\bar{\boldsymbol{x}}) \neq 0$, 则

$$\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}_i/\mathbb{U} \cup \{D\}). \tag{4.4.3}$$

否则 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U})$. 所以, 在每种情形 $\bar{\boldsymbol{x}}$ 都属于 (4.4.2) 式的右边.

另一方面, 设 $\bar{\boldsymbol{x}}$ 属于 (4.4.2) 式的右边. 如果 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U})$, 则显然有 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}/\mathbb{U})$. 否则, 存在 i, 使得 (4.4.3) 成立, 因此 $F_i(\bar{\boldsymbol{x}}) = 0$ 而 $D(\bar{\boldsymbol{x}}) \neq 0$. 故由 (4.3.5) 式得 $T_k(\bar{\boldsymbol{x}}) = 0$. 于是 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}/\mathbb{U})$. □

注 4.4.3 如果特别有 $D \in \mathcal{K}$ 或 $\dim(\mathbb{T}^{\{k-1\}}) = 0$, 那么 (4.4.2) 可简化为

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{t} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}).$$

这对 $D \in \mathcal{K}$ 是平凡的. 若 $\dim(\mathbb{T}^{\{k-1\}}) = 0$, 则由命题 4.5.10 有

$$\mathrm{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U}) = \emptyset, \quad \mathrm{Zero}(\mathbb{T}_i/\mathbb{U} \cup \{D\}) = \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}).$$

下面的算法推广了算法 IrrCharSer. 它所使用的策略源自文献 [97], 与 IrrCharSer 中用到的策略有所不同.

算法 IrrCharSerE: $\Psi \leftarrow \mathrm{IrrCharSerE}(\mathbb{P},\mathbb{Q})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P},\mathbb{Q}]$, 本算法计算 $[\mathbb{P},\mathbb{Q}]$ 的不可约特征序列 Ψ.

I1. 命 $\Phi \leftarrow \{[\mathbb{P},\mathbb{Q}]\}$, $\Psi \leftarrow \emptyset$.

I2. 重复下列步骤直至 $\Phi = \emptyset$:

I2.1. 设 $[\mathbb{F},\mathbb{G}]$ 为 Φ 中的元素, 且命 $\Phi \leftarrow \Phi \setminus \{[\mathbb{F},\mathbb{G}]\}$.

I2.2. 计算 $\mathbb{C} \leftarrow \mathrm{CharSet}(\mathbb{F})$.

I2.3. 若 $\mathbb{C}$ 为非矛盾列, 则:

I2.3.1. 命 $\mathbb{I} \leftarrow \mathrm{ini}(\mathbb{C}) \setminus \mathcal{K}$, $\Phi \leftarrow \Phi \cup \{[\mathbb{F} \cup \mathbb{C} \cup \{I\},\mathbb{G}]\colon\ I \in \mathbb{I}\}$.

I2.3.2. 计算 $[k,D,\mathbb{H}] \leftarrow \mathrm{Factor}(\mathbb{C})$. 若 $k=0$, 则转至 I2.3.3. 命

$$\begin{aligned}\Phi \leftarrow \Phi \cup \{[\mathbb{C} \setminus \{\mathrm{op}(k,\mathbb{C})\} \cup \{H\},\mathbb{G} \cup \mathbb{I} \cup \{D\}]\colon\ H \in \mathbb{H}\}\\ \cup\ \{[\mathbb{F} \cup \{D\},\mathbb{G} \cup \mathbb{I}]\}\end{aligned}$$

并转至 I2.

I2.3.3. 计算 $\mathbb{D} \leftarrow \mathrm{prem}(\mathbb{G} \cup \mathbb{I},\mathbb{C})$. 若 $0 \notin \mathbb{D}$, 则命 $\Psi \leftarrow \Psi \cup \{[\mathbb{C},\mathbb{D}]\}$.

由于对分解树的每个分支逐次添加的多项式组的基列的秩都严格递减, 上述算法显然终止. 它的正确性由前面的讨论可知.

使用引理 4.4.2 中的记号, 且命 $\mathbb{U}_i = \mathrm{prem}(\mathbb{U} \cup \{D\},\mathbb{T}_i)$ (这里伪除实际上只需对 $\mathbb{T}_i^{\{k\}} = [T_1,\cdots,T_{k-1},F_i]$ 进行). 如果 $0 \in \mathbb{U}_i$ 对某个 i 成立, 那么 (4.4.2) 中相应的分支可以抹去. 对于 $\mathbb{U}_i$ 不含有 0 的那些分支, 容易看出 $[\mathbb{T}_i,\mathbb{U}_i]$ 仍是良好三角系统; 特别对每个 i, $\mathbb{T}_i^{\{k\}}$ 都是不可约的. 而且, 所有 $\mathbb{T}_i$ 都与 $\mathbb{T}$ 有相同的参量.

多项式组 $\{D\} \cup \mathbb{T}$ 不一定具有三角形, 但可以将算法 QuaIrrTriSer 用于

$$[\{T_1,\cdots,T_q,D\},\mathbb{U},[T_{q+1},\cdots,T_r]]$$

使其三角化, 这里 q 是使 $\mathrm{cls}(T_q) \leq \mathrm{cls}(D)$ 的最大下标.

在下述算法步骤 D2.2.3 中, 次序对有序集合中元素的列举是按照自然的方式保持的. 譬如, 对 $\mathbb{S} = [1,\cdots,10]$ 有 $[i \in \mathbb{S}\colon\ 4 \leq i < 8, 2 \mid i] = [4,6]$.

算法 Decom: $[\Psi, \Phi] \leftarrow \mathrm{Decom}(\mathbb{T}, \mathbb{U})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中良好的拟不可约三角系统 $[\mathbb{T}, \mathbb{U}]$, 本算法计算两个集合

$$\Psi = \{[\mathbb{T}_1, \mathbb{U}_1], \cdots, [\mathbb{T}_e, \mathbb{U}_e]\}, \quad \Phi = \{[\mathbb{P}_1, \mathbb{Q}_1, \mathbb{T}_1^*], \cdots, [\mathbb{P}_h, \mathbb{Q}_h, \mathbb{T}_h^*]\},$$

使得

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i) \cup \bigcup_{j=1}^{h} \mathrm{Zero}(\mathbb{P}_j \cup \mathbb{T}_j^*/\mathbb{Q}_j), \tag{4.4.4}$$

这里每个 $[\mathbb{T}_i, \mathbb{U}_i]$ 都是不可约三角系统, $\mathbb{T}_i$ 与 $\mathbb{T}$ 具有相同的参量, $[\mathbb{P}_j, \mathbb{Q}_j, \mathbb{T}_j^*]$ 均为三元组, 而 $[\mathbb{T}_j^*, \mathbb{Q}_j]$ 构成良好的拟不可约三角系统. 在 $\Psi = \Phi = \emptyset$ 时 $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \emptyset$.

D1. 命 $\Phi \leftarrow \emptyset$, $r \leftarrow |\mathbb{T}|$. 若 $r = 1$, 则命 $\Psi \leftarrow \{[\mathbb{T}, \mathbb{U}]\}$, 且算法终止; 否则, 命 $\Omega \leftarrow \{[[\mathrm{op}(1, \mathbb{T})], \mathbb{T} \setminus [\mathrm{op}(1, \mathbb{T})], \mathbb{U}]\}$.

D2. 对 $i = 2, \cdots, r$ 执行下列步骤:

D2.1. 命 $\Psi \leftarrow \emptyset$.

D2.2. 对每个 $[\mathbb{T}', \mathbb{T}'', \mathbb{U}'] \in \Omega$ 执行下列步骤:

D2.2.1. 命 $T \leftarrow \mathrm{op}(1, \mathbb{T}'')$, $\mathbb{T}'' \leftarrow \mathbb{T}'' \setminus [T]$.

D2.2.2. 计算 $[k, D, \mathbb{F}] \leftarrow \mathrm{Factor}(\mathbb{T}' \cup [T])$. 若 $k = 0$, 则命 $D \leftarrow 1$, $\mathbb{F} \leftarrow \{T\}$.

D2.2.3. 命

$$\mathbb{T}^- \leftarrow [T' \in \mathbb{T}' : \ \mathrm{cls}(T') \le \mathrm{cls}(D)],$$
$$\mathbb{T}^+ \leftarrow [T' \in \mathbb{T}' : \ \mathrm{cls}(T') > \mathrm{cls}(D)].$$

若 $D \notin \mathcal{K}$ 且 $\mathbb{T}^- = \emptyset$ 或 $\dim(\mathbb{T}^-) > 0$, 则命

$$\Phi \leftarrow \Phi \cup \{[\mathbb{T}^- \cup \{D\}, \mathbb{U}', \mathbb{T}^+ \cup [T] \cup \mathbb{T}'']\}, \quad \mathbb{U}' \leftarrow \mathbb{U}' \cup \{D\}.$$

D2.2.4. 对每个 $F \in \mathbb{F}$ 执行:

D2.2.4.1. 命 $\mathbb{U}'' \leftarrow \mathrm{prem}(\mathbb{U}', \mathbb{T}' \cup [F])$.

D2.2.4.2. 若 $0 \notin \mathbb{U}''$, 则命 $\Psi \leftarrow \Psi \cup \{[\mathbb{T}' \cup [F], \mathbb{T}'', \mathbb{U}'']\}$.

D2.3. 命 $\Omega \leftarrow \Psi$.

D3. 命 $\Psi \leftarrow \{[\mathbb{T}', \mathbb{U}'] : \ [\mathbb{T}', \emptyset, \mathbb{U}'] \in \Psi\}$.

证　该算法中没有递归循环，因而终止性是平凡的. 算法的正确性由引理 4.4.2 和注 4.4.3 可得. □

顺便提及，因子分解步骤 D2.2.2 中的整数 k 只能是 0 或 $\imath$ (因为 $\mathbb{T}'$ 是不可约的，且长度为 $\imath - 1$).

例 4.4.2　考虑例 4.3.1 中求得的三角系统 $[\mathbb{T}_3', \mathbb{U}_3']$. 可以验证 $\mathbb{T}_3'$ 中的第二个多项式在以 $T_1 = t^2 + t + 1$ 为添加多项式从 Q 所得的代数扩域上有因子分解

$$-z^5 + t \doteq (z + t + 1)\, T_2, \tag{4.4.5}$$

其中

$$T_2 = -z^4 + tz^3 + z^3 - tz^2 - z + t + 1.$$

将多项式 $-z^5 + t$ 分别用其因子来替代，我们得到两个三角系统 $[\mathbb{T}_3^*, \mathbb{U}_3^*]$ 与 $[\mathbb{T}_3^{**}, \mathbb{U}_3^{**}]$, 其中

$$\begin{aligned} \mathbb{T}_3^* &= [T_1, z + t + 1, T_3, T_4], & \mathbb{T}_3^{**} &= [T_1, T_2, T_3, T_4], \\ \mathbb{U}_3^* &= \{t + 1\}, & \mathbb{U}_3^{**} &= \{z\}, \end{aligned}$$

而

$$T_3 = -z^3 y - t^3, \quad T_4 = zx^2 - t.$$

由于 T_3 关于 y 是线性的 (因而是不可约的), 我们只需检查 T_4 在代数扩域 $\mathrm{Q}(t, z)$ 上是否不可约，这里 $\mathrm{Q}(t, z)$ 是从 Q 分别以 $[T_1, z + t + 1]$ 和 $[T_1, T_2]$ 为添加三角列扩充而得. 使用代数因子分解，可以确定它是可约的，并分别有下列因子分解：

$$T_4 \doteq -(t + 1)\,(x + t)\,(x - t), \tag{4.4.6}$$

$$T_4 \doteq \frac{z}{D} T_4' T_4'', \tag{4.4.7}$$

其中

$$\begin{aligned} D &= 4\,tz^3 + 2\,z^3 + tz^2 + 2\,z^2 + tz - 2\,z + 3\,t, \\ T_4' &= z^3x + z^2x + tx + x + tz^3 + z^3 + z^2 - z + 2\,t + 1, \\ T_4'' &= tz^3x + 2\,z^3x - tz^2x + tzx + tx + x - tz^3 - z^3 - tz - t; \end{aligned}$$

因子 $t+1$, z 和分母都看作 $\mathbb{Q}(t,z)$ 中的元素. 将 $\mathbb{T}_3^*$ 和 $\mathbb{T}_3^{**}$ 中的 T_4 分别用导元为 x 的两个因子来替代, 我们得到四个不可约三角系统 $[\mathbb{T}_{3i},\mathbb{U}_{3i}]$, 这里

$$
\begin{aligned}
&\mathbb{T}_{31}=[T_1,z+t+1,T_3,x+t], && \mathbb{T}_{32}=[T_1,z+t+1,T_3,x-t],\\
&\mathbb{T}_{33}=[T_1,T_2,T_3,T_4'], && \mathbb{T}_{34}=[T_1,T_2,T_3,T_4''],\\
&\mathbb{U}_{31}=\mathbb{U}_{32}=\{t+1\}, && \mathbb{U}_{33}=\mathbb{U}_{34}=\{z\}.
\end{aligned}
$$

因此 $[\mathbb{T}_3',\mathbb{U}_3']$ 分解为四个不可约三角系统 $[\mathbb{T}_{31},\mathbb{U}_{31}],\cdots,[\mathbb{T}_{34},\mathbb{U}_{34}]$, 它们构成集合 Ψ.

对应于 (4.3.5) 中 D 的多项式在 (4.4.5) 和 (4.4.6) 中为 1. 关于因子分解 (4.4.7), 由于对应于 $\mathbb{T}^-$ 的不可约三角列 $[T_1,T_2]$ 是 0 维的, 根据命题 4.5.10, 我们不必考虑将 D 添加到三角列中的情形. 所以 $\Phi=\emptyset$.

算法 IrrTriSer: $\Psi\leftarrow\mathrm{IrrTriSer}(\mathbb{P},\mathbb{Q})$. 任给 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P},\mathbb{Q}]$, 本算法计算 $[\mathbb{P},\mathbb{Q}]$ 的不可约三角序列 Ψ.

I1. 命 $\Psi\leftarrow\emptyset$, $\Phi\leftarrow\{[\mathbb{P},\mathbb{Q},\emptyset,0]\}$.

I2. 重复下列步骤直至 $\Phi=\emptyset$:

I2.1. 设 $[\mathbb{F},\mathbb{G},\mathbb{T},m]$ 为 Φ 中的元素, 且命 $\Phi\leftarrow\Phi\setminus\{[\mathbb{F},\mathbb{G},\mathbb{T},m]\}$.

I2.2. 计算 $\Psi'\leftarrow\mathrm{QuaIrrTriSer}(\mathbb{F},\mathbb{G},\mathbb{T})$.

I2.3. 对每个 $[\mathbb{T},\mathbb{U}]\in\Psi'$ 执行下列步骤:

若 $|\mathbb{T}|>m$, 则计算 $[\bar{\Psi},\bar{\Phi}]\leftarrow\mathrm{Decom}(\mathbb{T},\mathbb{U})$, 且命

$$\Psi\leftarrow\Psi\cup\bar{\Psi},\quad \Phi\leftarrow\Phi\cup\{[\bar{\mathbb{P}},\bar{\mathbb{Q}},\bar{\mathbb{T}},|\mathbb{T}|]:\ [\bar{\mathbb{P}},\bar{\mathbb{Q}},\bar{\mathbb{T}}]\in\bar{\Phi}\}.$$

证 为了说明循环 I2 终止, 我们考虑 (步骤 I2.1) 从 Φ 中任意选取的 $[\mathbb{F},\mathbb{G},\mathbb{T},m]$ 以及在步骤 I2.3 中添加到 Φ 的 $[\bar{\mathbb{P}},\bar{\mathbb{Q}},\bar{\mathbb{T}},\bar{m}]$. 此时 $\bar{m}>m$. 因为 $\bar{m}$ 是三角列中多项式的个数, 因而不可能大于 n, 所以循环必定终止.

现在证明, 对步骤 I2.3 中的每个 $[\mathbb{T},\mathbb{U}]\in\Psi'$, 若 $|\mathbb{T}|\le m$, 则 $\mathrm{Zero}(\mathbb{T}/\mathbb{U})=\emptyset$. 一旦这一点得到证明, IrrTriSer 的正确性从零点关系式 (4.3.2) 和 (4.4.4) 立即可得.

设 $[\mathbb{T},\mathbb{U}]\in\Psi$ 同步骤 I2.3 中一样, 那么对任意由 Decom 从 $[\mathbb{T},\mathbb{U}]$ 生成的三元组 $[\bar{\mathbb{P}},\bar{\mathbb{Q}},\bar{\mathbb{T}}]$, $\bar{\mathbb{P}}$ 都是从不可约三角列 $\mathbb{T}^-$ 通过添加单个多项式 D 扩大而得. 并且 $[\mathbb{T}^-,\bar{\mathbb{Q}}]$ 是三角系统. 从 Decom 的 D2.2.3 中三元组的构造可以看出

$$\mathrm{cls}(D)\begin{cases}<\mathrm{cls}(T),\ \forall T\in\bar{\mathbb{T}},\\ \ge\mathrm{cls}(T),\ \forall T\in\mathbb{T}^-,\end{cases}$$

$|\mathbb{T}^-|+|\bar{\mathbb{T}}|=|\mathbb{T}|$, 且 D 对 $\mathbb{T}^-$ 是约化的. 设由 QuaIrrTriSer 从 $[\bar{\mathbb{P}},\bar{\mathbb{Q}},\bar{\mathbb{T}}]$ 计算出的拟不可约三角系统为 $[\mathbb{T}_1^*,\mathbb{U}_1^*],\cdots,[\mathbb{T}_h^*,\mathbb{U}_h^*]$, 那么每个 $\mathbb{T}_i^*$ 都能写成 $\mathbb{T}_i'\cup\bar{\mathbb{T}}$, 使得

$$\operatorname{Zero}(\bar{\mathbb{P}}/\bar{\mathbb{Q}})=\bigcup_{i=1}^{h}\operatorname{Zero}(\mathbb{T}_i'/\mathbb{U}_i^*).$$

按照定理 6.1.11, 如果 $|\mathbb{T}_i^*|\leq|\mathbb{T}|$, 那么 $[\mathbb{T}_i^*,\mathbb{U}_i^*]$ 是不完美的, 即 $\operatorname{Zero}(\mathbb{T}_i^*/\mathbb{U}_i^*)=\emptyset$ 对每个 i 成立. 因而算法正确, 如所欲证. □

在步骤 I2.3 中排除 $|\mathbb{T}|\leq m$ 的情形对于 IrrTriSer 的终止性甚为关键. 我们推测这一情形从来不会发生, 但我们无法给出证明. 如果确实如此, 那么上述算法可以通过不考虑第四个元素 m 而稍加简化; 这时正确性是显然的. 如果在 I2.3 中不加“如果”条件, 那么算法的终止性可以通过要求“在 Decom D2.2.2 的 T 之代数因子分解中多项式 D 不含有 $\mathbb{T}'$ 的依量”而得到证明. 如果在代数因子分解时附加一些 (正规化) 计算, 该要求是能满足的.

例 4.4.3　我们再来考察例 2.3.2 和 4.3.1 中的三角系统. $[\mathbb{T}_2,\mathbb{U}_2]$ 的不可约性是平凡的. 代数因子分解表明 $[\mathbb{T}_1,\mathbb{U}_1]$ 也是不可约的. 正如我们在例 4.4.2 中已经看到, $[\mathbb{T}_3',\mathbb{U}_3']$ 可以分解为四个不可约三角系统. 容易发现 $[\mathbb{T}_3'',\mathbb{U}_3'']$ 是可约的; 这是因为将 $t=1$ 代入到 $\mathbb{T}_3''$ 的第二个多项式即导致可约的 z^5-1. 事实上, 用算法 Decom 也能将该三角系统分解为四个不可约三角系统 $[\mathbb{T}_{35},\mathbb{U}_{35}],\cdots,[\mathbb{T}_{38},\mathbb{U}_{38}]$, 其中

$$\begin{aligned}
\mathbb{T}_{35}&=[t-1,z-1,y+1,x-1],\\
\mathbb{T}_{36}&=[t-1,z-1,y+1,x+1],\\
\mathbb{T}_{37}&=[t-1,z^4+z^3+z^2+z+1,z^3y+1,x-z^2],\\
\mathbb{T}_{38}&=[t-1,z^4+z^3+z^2+z+1,z^3y+1,x+z^2],\\
\mathbb{U}_{35}&=\mathbb{U}_{36}=\emptyset,\\
\mathbb{U}_{37}&=\mathbb{U}_{38}=\{z\}.
\end{aligned}$$

我们将这一分解的细节略去.

总之, 原来的多项式组 $\mathbb{P}$ 已分解为 10 个不可约三角系统 $[\mathbb{T}_1,\mathbb{U}_1],[\mathbb{T}_2,\mathbb{U}_2],[\mathbb{T}_{31},\mathbb{U}_{31}],\cdots,[\mathbb{T}_{38},\mathbb{U}_{38}]$, 使得

$$\operatorname{Zero}(\mathbb{P})=\operatorname{Zero}(\mathbb{T}_1/\mathbb{U}_1)\cup\operatorname{Zero}(\mathbb{T}_2/\mathbb{U}_2)\cup\bigcup_{j=1}^{8}\operatorname{Zero}(\mathbb{T}_{3j}/\mathbb{U}_{3j}).$$

由定理 4.5.11 (b), 以上分解中的每个 $\mathbb{U}_i$ 都可以用 $\mathrm{ini}(\mathbb{T}_i)$ 来替换. 由于 $|\mathbb{T}_2| = |\mathbb{T}_{3j}| = 4$ (变元的个数), $1 \le j \le 8$, 按照命题 4.5.10 有

$$\mathrm{Zero}(\mathbb{T}_i/\mathrm{ini}(\mathbb{T}_i)) = \mathrm{Zero}(\mathbb{T}_i), \quad i = 2, 31, \cdots, 38.$$

所以

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{T}_1/\mathrm{ini}(\mathbb{T}_1)) \cup \mathrm{Zero}(\mathbb{T}_2) \cup \bigcup_{j=1}^{8} \mathrm{Zero}(\mathbb{T}_{3j}). \tag{4.4.8}$$

例 4.4.4 作为进一步的说明, 我们再来考虑一个较复杂的多项式系统 $\mathfrak{P} = [\{P_1, P_2, P_3\}, \{x_3\}]$, 其中

$$\begin{aligned}
P_1 &= x_3\,(x_5^2 - x_4^2 + 2\,x_1x_4 - x_1^2) + 2\,x_1\,(x_1 - x_4)\,x_5,\\
P_2 &= x_3\,(x_5^2 - x_4^2 + 2\,x_2x_4 - x_2^2) + 2\,x_2\,(x_2 - x_4)\,x_5,\\
P_3 &= x_3\,[(x_1 - x_6)\,(x_2x_6 + x_3^2) + (x_2 - x_6)\,(x_1x_6 + x_3^2)].
\end{aligned}$$

关于变元序 $x_1 \prec \cdots \prec x_6$, $\mathfrak{P}$ 可分解为 7 个 (约化的) 不可约三角列 $\mathbb{T}_i$, 使得

$$\mathrm{Zero}(\mathfrak{P}) = \bigcup_{i=1}^{7} \mathrm{Zero}(\mathbb{T}_i/\mathrm{ini}(\mathbb{T}_i) \cup \{x_3\}), \tag{4.4.9}$$

其中

$$\begin{aligned}
\mathbb{T}_1 &= [T_1, T_2, T_3],\\
\mathbb{T}_2 &= [T_1, T_2, T_3'],\\
\mathbb{T}_3 &= [x_2 + x_1, x_3^2 + x_1^2, x_4, x_5 - x_3],\\
\mathbb{T}_4 &= [x_2 + x_1, x_4^2 - x_3^2 - x_1^2, x_5 - x_3, x_6],\\
\mathbb{T}_5 &= [x_2 + x_1, x_4, x_3x_5^2 + 2\,x_1^2x_5 - x_1^2x_3, x_6],\\
\mathbb{T}_6 &= [x_2 - x_1, T_2', x_6 - x_1],\\
\mathbb{T}_7 &= [x_2 - x_1, T_2', x_1x_6 + x_3^2];\\
T_1 &= 4\,x_4^4 - 8\,(x_2 + x_1)\,x_4^3 - 4\,(x_3^2 - x_2^2 - 3\,x_1x_2 - x_1^2)\,x_4^2\\
&\quad + 4\,(x_2x_3^2 + x_1x_3^2 - x_1x_2^2 - x_1^2x_2)\,x_4 - (x_2^2 + 2\,x_1x_2 + x_1^2)\,x_3^2,\\
T_2 &= 2\,(x_4 - x_2 - x_1)\,x_5 - 2\,x_3x_4 + (x_2 + x_1)\,x_3,\\
T_2' &= x_3x_5^2 - 2\,x_1\,(x_4 - x_1)\,x_5 - x_3x_4^2 + 2\,x_1x_3x_4 - x_1^2x_3,\\
T_3 &= (x_2 + x_1)\,x_6 + 2\,x_4^2 - 2\,(x_2 + x_1)\,x_4,\\
T_3' &= (x_2 + x_1)\,x_6 - 2\,x_4^2 + 2\,(x_2 + x_1)\,x_4 + 2\,x_3^2 - 2\,x_1x_2.
\end{aligned}$$

4.5 不可约三角系统的性质

以下我们将 $(\boldsymbol{u}, y_1, \cdots, y_i)$ 写成 $\boldsymbol{z}_i$, $(\boldsymbol{u}, \eta_1, \cdots, \eta_i)$ 写成 $\boldsymbol{\xi}_i$, 而 $\boldsymbol{z} = \boldsymbol{z}_r$, $\boldsymbol{\xi} = \boldsymbol{\xi}_r$. 显然 $\boldsymbol{z}$ 是 $\boldsymbol{x}$ 的置换. 下述引理源自文献 [96] (171 和 172 页).

引理 4.5.1 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{z}]$ 中的不可约三角列, 而 $\boldsymbol{\xi}$ 为 $\mathbb{T}$ 的一般零点, 那么, 对任意多项式 $P \in \mathcal{K}[\boldsymbol{z}]$,

$$\operatorname{prem}(P, \mathbb{T}) = 0 \iff P(\boldsymbol{\xi}) = 0.$$

证 设 $\mathbb{T} = [T_1, \cdots, T_r]$ 和 (4.3.3) 中相同, 且

$$I_i = \operatorname{ini}(T_i),\ d_i = \operatorname{ldeg}(T_i),\quad 1 \le i \le r,$$

而 $\boldsymbol{\xi}$ 具有形式

$$\boldsymbol{\xi} = (\boldsymbol{u}, \eta_1, \cdots, \eta_r).$$

和以前一样, $\mathcal{K}_k = \mathcal{K}(\boldsymbol{\xi}_k)$. 我们首先证明下面的断言:

(A) 如果 $R \in \mathcal{K}[\boldsymbol{z}]$ 对 $\mathbb{T}$ 是约化的, 且 $R(\boldsymbol{\xi}) = 0$, 那么 $R \equiv 0$.

注意, η_r 是多项式

$$\bar{R} = R(\boldsymbol{\xi}_{r-1}, y_r),\quad \bar{T}_r = T_r(\boldsymbol{\xi}_{r-1}, y_r) \in \mathcal{K}_{r-1}[y_r]$$

的扩充零点. 由于 $\bar{T}_r$ 在 $\mathcal{K}_{r-1}$ 上不可约, 而 $\deg(R, y_r) < d_r$, 故 $\bar{R} \equiv 0$. 所以, 作为 y_r 的多项式 $\bar{R}$ 的所有系数都恒等于 0, 即

$$R_i(\boldsymbol{\xi}_{r-1}) = \operatorname{coef}(\bar{R}, y_r^i) \equiv 0,\quad 0 \le i < d_r.$$

类似地, η_{r-1} 是多项式

$$\bar{R}_i = R_i(\boldsymbol{\xi}_{r-2}, y_{r-1}),\quad \bar{T}_{r-1} = T_{r-1}(\boldsymbol{\xi}_{r-2}, y_{r-1}) \in \mathcal{K}_{r-2}[y_{r-1}]$$

的扩充零点. 由于 R 对 $\mathbb{T}$ 是约化的, 因而 R_i 也是. 所以 $\deg(R_i, y_{r-1}) < d_{r-1}$. 这与 $\bar{T}_{r-1}$ 在 $\mathcal{K}_{r-2}$ 上的不可约性一起表明 $\bar{R}_i \equiv 0$ 对所有 i 成立. 由此可知 $\bar{R}_i$ 关于 y_{r-1} 的系数也都恒等于 0, 因而 R_i 关于 y_{r-1} 的系数在用 $\boldsymbol{\xi}_{r-2}$ 替换 $\boldsymbol{z}_{r-2}$ 之后也是如此.

以上论证可对 $T_{r-2}, \cdots, T_1$ 继续. 这样下去, 我们将会看到, 作为 $\mathcal{K}_0[y_1, \cdots, y_r]$ 中的多项式 R 的所有系数都必须恒等于 0. 于是 $R \equiv 0$, 因而断言 (A) 获证.

为了完成引理 4.5.1 的证明，我们命 $R = \text{prem}(P, \mathbb{T})$，那么存在整数 $s_i \geq 0$ 和多项式 Q_i，使得

$$I_1^{s_1} \cdots I_r^{s_r} P = \sum_{i=1}^{r} Q_i T_i + R. \tag{4.5.1}$$

由于 $T_i(\boldsymbol{\xi}) = 0$，将 $\boldsymbol{\xi}$ 代入公式 (4.5.1) 得

$$I_1(\boldsymbol{\xi})^{s_1} \cdots I_r(\boldsymbol{\xi})^{s_r} P(\boldsymbol{\xi}) = R(\boldsymbol{\xi}).$$

因为每个 I_i 都是非零多项式且对 $\mathbb{T}$ 是约化的，故由断言 (A) 可知 $I_i(\boldsymbol{\xi}) \neq 0$. 所以

$$P(\boldsymbol{\xi}) = 0 \iff R(\boldsymbol{\xi}) = 0 \iff R = 0.$$

由于 R 对 $\mathbb{T}$ 是约化的，上面的第二个 " $\iff$ " 也由断言 (A) 保证. 证毕. □

引理 4.5.2 设 $\mathbb{T}, P, R, Q$ 等与引理 3.2.5 中相同. 如果 $\mathbb{T}$ 不可约，以

$$\boldsymbol{\xi} = (\boldsymbol{u}, \eta_1, \cdots, \eta_r)$$

为一般零点，并且 $\text{prem}(P, \mathbb{T}) \neq 0$，那么 $R(\boldsymbol{u}) \neq 0$, $Q(\boldsymbol{\xi}) \neq 0$.

证 命

$$R_r = \text{res}(P, T_r, y_r), \quad R_i = \text{res}(R_{i+1}, T_i, y_i), \quad i = r-1, \cdots, 1,$$

其中 $y_i = \text{lv}(T_i)$，而 $R_1 = R$. 由于 $\mathbb{T}$ 不可约，且 $\text{prem}(P, \mathbb{T}) \neq 0$，根据引理 4.5.1 有 $P(\boldsymbol{\xi}) \neq 0$. 另一方面，$\bar{T}_r = T_r(\boldsymbol{\xi}_{r-1}, y_r)$ 在 $\mathcal{K}(\boldsymbol{\xi}_{r-1})$ 上不可约，并且 $T_r(\boldsymbol{\xi}) = \bar{T}_r(\eta_r) = 0$. 因此，多项式 $P(\boldsymbol{\xi}_{r-1}, y_r)$ 和 $\bar{T}_r$ 关于 y_r 在 $\mathcal{K}(\boldsymbol{\xi}_{r-1})$ 的任意扩域中不可能有公共零点，所以

$$R_r(\boldsymbol{\xi}_{r-1}) \neq 0.$$

由于 $T_{r-1}(\boldsymbol{\xi}_{r-2}, y_{r-1})$ 在 $\mathcal{K}(\boldsymbol{\xi}_{r-2})$ 上不可约且 $T_{r-1}(\boldsymbol{\xi}_{r-1}) = 0$，基于同样的理由我们有 $R_{r-1}(\boldsymbol{\xi}_{r-2}) \neq 0$. 继续这种论证，最终我们将有

$$R(\boldsymbol{u}) = R_1(\boldsymbol{u}) \neq 0.$$

将 $\boldsymbol{\xi}$ 代入 (3.2.4) 中的多项式，立即得到 $Q(\boldsymbol{\xi}) \neq 0$. 引理获证. □

关于引理 4.5.2 的另一个证明，参阅 [96] (第 172 至 174 页). 下述定理及其证明亦源自吴的著作 [96] (185 至 187 页).

定理 4.5.3 $\mathcal{K}[\boldsymbol{x}]$ 中的每个不可约三角系统在 $\mathcal{K}$ 的代数闭包 $\bar{\mathcal{K}}$ 上都是完美的.

证 设 $[\mathbb{T},\mathbb{U}]$ 为不可约三角系统，其中 $\mathbb{T}=[T_1,\cdots,T_r]$ 写成 (4.3.3) 的形式. 又命

$$I_i=\mathrm{ini}(T_i),\ 1\le i\le r,\quad 且\ V=\prod_{U\in\mathbb{U}}U.$$

因 $\mathrm{prem}(I_i,\mathbb{T}^{\{i-1\}})\neq 0$, 故由引理 3.2.5 和 4.5.2, 存在多项式 $Q_i,Q_{ij}\in\mathcal{K}[\boldsymbol{z}_{i-1}]$, 使得

$$R_i=Q_iI_i-\sum_{j=1}^{i-1}Q_{ij}T_j\in\mathcal{K}[\boldsymbol{u}],$$

且对每个 i 都有 $R_i\neq 0$. 由于 $\mathrm{prem}(U,\mathbb{T})\neq 0$ 对任意 $U\in\mathbb{U}$ 成立，根据引理 4.5.1 有 $\mathrm{prem}(V,\mathbb{T})\neq 0$. 再由引理 3.2.5 和 4.5.2, 存在多项式 $H,H_i\in\mathcal{K}[\boldsymbol{z}]$, 使得

$$R=HV-\sum_{i=1}^{r}H_iT_i\in\mathcal{K}[\boldsymbol{u}],\tag{4.5.2}$$

且 $R\neq 0$. 所以，存在一点 $\bar{\boldsymbol{u}}=(\bar{u}_1,\cdots,\bar{u}_d)\in\mathcal{K}^d$, 使得

$$R_1(\bar{\boldsymbol{u}})\cdots R_r(\bar{\boldsymbol{u}})R(\bar{\boldsymbol{u}})\neq 0.$$

这样的 $\bar{\boldsymbol{u}}$ 可选为有理点.

现在我们用归纳法确定 $\bar{y}_i\in\bar{\mathcal{K}}$, 使得点

$$\bar{\boldsymbol{z}}=(\bar{\boldsymbol{u}},\bar{y}_1,\cdots,\bar{y}_r)\in\bar{\mathcal{K}}^{d+r}$$

满足下列关系:

$$T_i(\bar{\boldsymbol{z}}_i)=0,\quad I_{i+1}(\bar{\boldsymbol{z}}_i)\neq 0.\tag{4.5.3}$$

首先，命

$$\bar{T}_1=T_1(\bar{\boldsymbol{u}},y_1)\in\mathcal{K}[y_1],\quad \bar{I}_1=I_1(\bar{\boldsymbol{u}})\in\mathcal{K}.$$

因为

$$Q_1(\bar{\boldsymbol{u}})I_1(\bar{\boldsymbol{u}})=R_1(\bar{\boldsymbol{u}})\neq 0,$$

所以 $\bar{I}_1 \neq 0$, 而 $\bar{T}_1$ 是关于 y_1 次数 ≥ 1 的多项式. 因此, 可以从 $\mathcal{K}$ 的某一代数扩域中选取 $\bar{y}_1$, 使得

$$\bar{T}_1(\bar{y}_1) = 0, \quad 或 \quad T_1(\bar{z}_1) = 0.$$

由于

$$R_2 = Q_2 I_2 - Q_{21} T_1, \quad R_2(\bar{z}_1) = R_2(\bar{u}) \neq 0,$$

我们有 $I_2(\bar{z}_1) \neq 0$. 故 (4.5.3) 对 $i = 1$ 成立.

假设我们已经求得 $\bar{y}_1, \cdots, \bar{y}_i$ 满足 (4.5.3), 今欲求 $\bar{y}_{i+1}$.

为此, 命

$$\bar{T}_{i+1} = T_{i+1}(\bar{z}_i, y_{i+1}) \in \mathcal{K}'[y_{i+1}],$$

其中 $\mathcal{K}'$ 是 $\mathcal{K}$ 的某一包含 $\bar{y}_1, \cdots, \bar{y}_i$ 的代数扩域. 看作 y_{i+1} 的多项式, $\bar{T}_{i+1}$ 的导系数为 $I_{i+1}(\bar{z}_i) \neq 0$. 于是在 $\mathcal{K}'$ 因而 $\mathcal{K}$ 的某一代数扩域中可以选取 $\bar{y}_{i+1}$, 使得 $\bar{T}_{i+1}(\bar{y}_{i+1}) = 0$ 或 $T_{i+1}(\bar{z}_{i+1}) = 0$. 所以

$$R_{i+2} = Q_{i+2} I_{i+2} - \sum_{j=1}^{i+1} Q_{i+2\ j} T_j,$$

$$R_{i+2}(\bar{z}_{i+1}) = R_{i+2}(\bar{u}) \neq 0,$$

而

$$T_1(\bar{z}_{i+1}) = T_1(\bar{z}_1) = 0, \cdots, T_{i+1}(\bar{z}_{i+1}) = 0$$

蕴涵着 $I_{i+2}(\bar{z}_{i+1}) \neq 0$. 最后, 将以上构造的 $\bar{z}$ 代入 (4.5.2) 式可得 $V(\bar{z}) \neq 0$; 因此 $\bar{z}$ 是 $[\mathbb{T}, \mathbb{U}]$ 的零点. 定理证毕. □

推论 4.5.4 $\mathcal{K}[\boldsymbol{x}]$ 中的每个不可约三角列在 $\mathcal{K}$ 的代数闭包 $\bar{\mathcal{K}}$ 上都是完美的.

推论 4.5.5 $\mathcal{K}[\boldsymbol{x}]$ 中的任意不可约三角列和系统都是完美的.

事实上, 推论 4.5.5 的建立也可以不用定理 4.5.3. 这是因为不可约三角列 $\mathbb{T}$ 的一般零点也是 $[\mathbb{T}, \mathrm{ini}(\mathbb{T})]$ 以及任意良好三角系统 $[\mathbb{T}, \mathbb{U}]$ 在 $\mathcal{K}$ 的某一扩域中的零点.

推论 4.5.6 设 Ψ 为 $\mathcal{K}[\boldsymbol{x}]$ 中多项式系统 $\mathfrak{P}$ 的不可约三角序列, 那么

$$\mathrm{Zero}(\mathfrak{P}) = \emptyset \iff \Psi = \emptyset.$$

命题 4.5.7 $\mathcal{K}[\boldsymbol{x}]$ 中的每个不可约三角列都是简单列.

证 设 $\mathbb{T}=[T_1,\cdots,T_r]$ 为一不可约三角列，写成 (4.3.3) 的形式，且

$$I_i=\mathrm{ini}(T_i),\quad T_i'=\frac{\partial T_i}{\partial y_i},\ 1\le i\le r.$$

又命

$$D=I_1\cdots I_rT_1'\cdots T_r'.$$

由于 $\mathrm{prem}(I_i,\mathbb{T})\neq 0$, $\mathrm{prem}(T_i',\mathbb{T})\neq 0$ 对所有 i 成立，故 $\mathrm{prem}(D,\mathbb{T})\neq 0$. 由引理 3.2.5 和 4.5.2, 存在多项式 $Q,Q_i\in\mathcal{K}[\boldsymbol{z}]$, 使得

$$R=\mathrm{res}(D,\mathbb{T})=QD-\sum_{i=1}^{r}Q_iT_i\neq 0, \tag{4.5.4}$$

且 $R\in\mathcal{K}[\boldsymbol{u}]$. 命 $\tilde{T}_t=\mathrm{sqfr}(R)$, 这里 $\mathrm{sqfr}(R)$ 表示 R 在 $\mathcal{K}$ 上所有互异不可约因子的乘积 (即 R 的最大无平方因子), 而下标 t 则按如下方式确定. 构造 $t-1$ 个多项式

$$\tilde{T}_{i-1}=\mathrm{sqfr}\left(\mathrm{ini}(\tilde{T}_i)\,\mathrm{res}\left(\tilde{T}_i,\frac{\partial\tilde{T}_i}{\partial u_{p_i}},u_{p_i}\right)\right),\quad i=t,\cdots,2,$$

使得

$$\tilde{T}_0=\mathrm{ini}(\tilde{T}_1)\,\mathrm{res}\left(\tilde{T}_1,\frac{\partial\tilde{T}_1}{\partial u_{p_1}},u_{p_1}\right)\in\mathcal{K},$$

这里 $u_{p_i}=\mathrm{lv}(\tilde{T}_i)$, 且对每个 i 有 $\tilde{T}_i\neq 0$. 令 $\tilde{\mathbb{T}}=[\tilde{T}_1,\cdots,\tilde{T}_t]$. 今欲证 $[\mathbb{T},\tilde{\mathbb{T}}]$ 为简单系统. 从 $\tilde{T}_i$ 的构造容易看出，对任意 $\bar{\boldsymbol{u}}^{\{p_i-1\}}\in\mathrm{Zero}(\emptyset/\tilde{\mathbb{T}}^{\{i-1\}})$ 有

$$\mathrm{ini}(\tilde{T}_i)(\bar{\boldsymbol{u}}^{\{p_i-1\}})\neq 0,\quad \text{且}\quad \tilde{T}_i(\bar{\boldsymbol{u}}^{\{p_i-1\}},u_{p_i})\ \text{无平方因子}.$$

现命

$$\bar{\boldsymbol{z}}_{i-1}=(\bar{\boldsymbol{u}},\bar{\boldsymbol{y}}_{i-1})\in\mathrm{Zero}(\mathbb{T}^{\{i-1\}}/\tilde{\mathbb{T}}).$$

显然 $R(\bar{\boldsymbol{z}}_{i-1})=R(\bar{\boldsymbol{u}})\neq 0$. 为了说明 $T_i(\bar{\boldsymbol{z}}_{i-1},y_i)$ 无平方因子，我们假设不是如此：即 $T_i(\bar{\boldsymbol{z}}_{i-1},y_i)$ 与 $T_i'(\bar{\boldsymbol{z}}_{i-1},y_i)$ 有一关于 y_i 次数 ≥ 1 的公因子，由此导出矛盾. 按照假设，存在 $\bar{y}_i\in\tilde{\mathcal{K}}$, 使得

$$T_i(\bar{\boldsymbol{z}}_i)=T_i'(\bar{\boldsymbol{z}}_i)=0.$$

由此即知，对任意 $\bar{y}_{i+1},\cdots,\bar{y}_r \in \tilde{\mathcal{K}}$ 有 $D(\bar{z}_i,\bar{y}_{i+1},\cdots,\bar{y}_r)=0$. 很明显，该结论在 $I_i(\bar{z}_{i-1})=0$ 时也成立.

另一方面，因 $\mathbb{T}$ 不可约，故由推论 4.5.5, 存在 $\bar{y}_{i+1},\cdots,\bar{y}_r \in \tilde{\mathcal{K}}$, 使得

$$I_j(\bar{z}) \neq 0,\ T_j(\bar{z})=0,\quad j>i.$$

将 $\bar{z}$ 代入 (4.5.4) 得 $D(\bar{z}) \neq 0$. 由此导致矛盾. 所以

$$I_i(\bar{z}_{i-1}) \neq 0,\quad \text{且}\ T_i(\bar{z}_{i-1},y_i)\ \text{无平方因子}.$$

因而 $[\mathbb{T},\tilde{\mathbb{T}}]$ 是简单系统. 如所欲证. □

上述命题的另一个较简单的证明可由引理 5.2.1 给出.

粗略地说，简单列是特殊的三角列 $\mathbb{T}$, 其中每个多项式关于其导元 x_p 在所有从 $\mathcal{K}$ —— 以 $\mathbb{T}^{\{p-1\}}$ 的不可约分支为添加三角列 —— 所得的代数扩域上都无平方因子. 一个不可约三角系统并不一定是简单系统. 这一点可以从例 3.3.2 中的三角系统 $[\mathbb{T}_1,\{T\}]$ 看出：尽管 $\mathbb{T}_1$ 不可约，但 $[\mathbb{T}_1,\{T\}]$ 并不是简单系统.

由推论 3.4.5 和命题 4.5.7 可得：

推论 4.5.8 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意不可约三角列 $\mathbb{T}$ 与多项式 P,

$$\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})) \subset \mathrm{Zero}(P) \iff \mathrm{prem}(P,\mathbb{T})=0.$$

以下推论与定理 3.4.4 相对应.

推论 4.5.9 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意不可约三角系统 $[\mathbb{T},\mathbb{U}]$ 与多项式 P,

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(P) \iff \mathrm{prem}(P,\mathbb{T})=0.$$

证 因 $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T}))$, 故 “$\Longleftarrow$” 由推论 4.5.8 即得.

欲证另一方向, 设 $\boldsymbol{\xi}$ 为 $\mathbb{T}$ 的一般零点. 对任意 $U \in \mathbb{U}$, 由于 $\mathrm{prem}(U,\mathbb{T}) \neq 0$, 依引理 4.5.1 有 $U(\boldsymbol{\xi}) \neq 0$. 由此可知

$$\boldsymbol{\xi} \in \mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(P).$$

因而 $P(\boldsymbol{\xi})=0$. 再应用引理 4.5.1 即得 $\mathrm{prem}(P,\mathbb{T})=0$. □

命题 4.5.10 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的不可约三角列，P 为多项式，且 $\operatorname{prem}(P, \mathbb{T}) \neq 0$. 若 $\dim(\mathbb{T}) = 0$, 则

$$\operatorname{Zero}(\{P\} \cup \mathbb{T}) = \emptyset, \quad \operatorname{Zero}(\mathbb{T}/\mathbb{I}) = \operatorname{Zero}(\mathbb{T}),$$

其中 $\mathbb{I} = \operatorname{ini}(\mathbb{T})$.

证 第一个等式由引理 3.2.5 和 4.5.2 即得. 由于

$$\operatorname{Zero}(\mathbb{T}) = \operatorname{Zero}(\mathbb{T}/\mathbb{I}) \cup \bigcup_{I \in \mathbb{I}} \operatorname{Zero}(\{I\} \cup \mathbb{T}),$$

第二个等式也很显然. □

在由特征列方法计算的形如 (2.2.7) 的零点分解中，$\operatorname{Zero}(\mathbb{C}_i/\operatorname{ini}(\mathbb{C}_i) \cup \mathbb{Q})$ 代替了三角序列零点分解中的 $\operatorname{Zero}(\mathbb{T}_i/\mathbb{U}_i)$, 这里每个 $\mathbb{C}_i$ 都是升列，且有 $\operatorname{prem}(\mathbb{P}, \mathbb{C}_i) = \{0\}$ 和 $0 \notin \operatorname{prem}(\mathbb{Q}, \mathbb{C}_i)$ 这两条性质. 一般来说，$\operatorname{prem}(\mathbb{P}, \mathbb{T}_i) = \{0\}$ 是没有保证的，并且每个 $\mathbb{U}_i$ 可能比 $\operatorname{ini}(\mathbb{C}_i) \cup \mathbb{Q}$ 含有多得多的多项式. 值得重提的是，如果三角序列是不可约或简单的，那么性质 $\operatorname{prem}(\mathbb{P}, \mathbb{T}_i) = \{0\}$ 便可恢复.

与简单序列的定理 3.4.6 平行，我们将有关不可约三角序列的这些性质叙述成如下定理. 这里应用推论 4.5.9 容易证明性质 (a), 而 (b) 的证明与定理 3.4.6 (b) 的证明相仿.

定理 4.5.11 设 Ψ 为 $\mathcal{K}[\boldsymbol{x}]$ 中任一多项式系统 $[\mathbb{P}, \mathbb{Q}]$ 的不可约三角序列，那么

(a) $\operatorname{prem}(\mathbb{P}, \mathbb{T}) = \{0\}$ 与 $0 \notin \operatorname{prem}(\mathbb{Q}, \mathbb{T})$ 对所有 $[\mathbb{T}, \mathbb{U}] \in \Psi$ 成立；

(b)

$$\operatorname{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{[\mathbb{T},\mathbb{U}] \in \Psi} \operatorname{Zero}(\mathbb{T}/\operatorname{ini}(\mathbb{T}) \cup \mathbb{Q}). \tag{4.5.5}$$

若 $\dim(\mathbb{T}) = 0$, 则 (4.5.5) 中的 $\operatorname{Zero}(\mathbb{T}/\operatorname{ini}(\mathbb{T}) \cup \mathbb{Q})$ 可简化为 $\operatorname{Zero}(\mathbb{T}/\mathbb{Q})$.

证 (a) 设 $[\mathbb{T}, \mathbb{U}] \in \Psi$, 那么 $\operatorname{Zero}(\mathbb{T}/\mathbb{U}) \subset \operatorname{Zero}(\mathbb{P}/\mathbb{Q})$. 于是对所有 $P \in \mathbb{P}$ 与 $Q \in \mathbb{Q}$ 有

$$\operatorname{Zero}(\mathbb{T}/\mathbb{U}) \subset \operatorname{Zero}(P), \quad \operatorname{Zero}(\mathbb{T}/\mathbb{U}) \not\subset \operatorname{Zero}(Q),$$

因此由推论 4.5.9 可知

$$\mathrm{prem}(P, \mathbb{T}) = 0, \quad \mathrm{prem}(Q, \mathbb{T}) \neq 0.$$

(b) 依据 (a) 和伪余公式，任意属于 (4.5.5) 式右边的 $\boldsymbol{x}$ 都包含于其左边. 反之，设 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. 根据定义存在 $[\mathbb{T}, \mathbb{U}] \in \Psi$，使得 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}/\mathbb{U})$. 因 $[\mathbb{T}, \mathbb{U}]$ 为三角系统，故对任意 $I \in \mathrm{ini}(\mathbb{T})$ 有 $I(\bar{\boldsymbol{x}}) \neq 0$. 所以 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T}) \cup \mathbb{Q})$，即 $\bar{\boldsymbol{x}}$ 属于 (4.5.5) 式的右边. 若 $\dim(\mathbb{T}) = 0$，则依命题 4.5.10, $\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T}) \cup \mathbb{Q})$ 可简化为 $\mathrm{Zero}(\mathbb{T}/\mathbb{Q})$. □

在定理 4.5.11 中，每个不可约三角系统 $[\mathbb{T}, \mathbb{U}] \in \Psi$ 都满足性质 (a)，无论 Ψ 中的其他三角系统可约与否. 在基于特征列的分解算法中，该性质可用来避免某些 0 伪余式的验证.

推论 4.5.12 $\mathcal{K}[\boldsymbol{x}]$ 中多项式系统 $\mathfrak{P}$ 的任意不可约三角序列都是 $\mathfrak{P}$ 的不可约 W 特征序列.

设 $\mathbb{T}$ 为正则列，如 (3.2.1) 所示，其中 $d_i = \mathrm{ldeg}(T_i)$, $d = d_1 \cdots d_r$, $\mathbb{T}$ 自然是完美的. 如果 $\mathbb{T}$ 不可约，那么它有 d 个互异的正则零点；这些零点也称为 $\mathbb{T}$ 的 *一般零点*，它们生成 $\mathcal{K}$ 的同一扩域. 如果 $\mathbb{T}$ 是简单但可约的，那么它也有 d 个互异的正则零点；这些零点生成至少两个 $\mathcal{K}$ 的、具有相同超越次数的扩域. 如果 $\mathbb{T}$ 是可约的但不是简单的，那么它有少于 d 个互异的正则零点；这些零点生成一个或者多个 $\mathcal{K}$ 的、具有相同超越次数的扩域.

上面的说明有助于理解正则列、简单列和不可约三角列之间的不同之处. 术语“正则零点”是卡尔克布伦纳在文献 [35] 中对正则列引进的；在 3.2 节中它已被用于任意三角系统. 我们可以将正则零点理解为“一般零点”，但后一概念已在代数几何中专用于不可约代数簇及其相应的不可约三角列.

本节中的部分结果是 3.4 节中有关简单系统性质的推论. 其他新证的有关不可约三角列或系统的结果大多对简单列或系统同样成立，或者能被推广. 当然需要适当更换相应的概念. 这些结果包括引理 4.5.1 和 4.5.2, 定理 4.5.3, 以及命题 4.5.10 中的性质. 定理 4.5.3 的一个推广已作为定理 3.2.13 给出. 其他结果的推广将另文论述.

第五章 典范三角列、格罗布讷基与结式法

将基于结式和格罗布讷基的消去法推迟到本章来介绍有些异乎寻常. 原因是这些方法已很著名, 并见诸于标准教科书, 因而易于查阅. 为了减少重复文献中已有的材料, 我们不再仔细讨论这些方法, 而只对它们作一个简略的回顾. 大多数结果的证明都将略去.

如读者所知, 我们的重点是系统介绍基于伪除的消去技术. 目的是建立多元多项式的零点集 (而不是理想) 的各种分解. 这一偏重将在本章的前一半中继续.

5.1 典范三角列

引进正则列的收获之一是推论 3.2.7, 它保证了, 对任意正则但可能可约的三角列 $\mathbb{T}$, 零点集 $\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T}))$ 都非空. 现在, 我们希望对三角列附加更多的限制, 但非不可约性, 而使其典范化.

定义 5.1.1 $\mathcal{K}[\boldsymbol{x}]$ 中的三角系统 $[\mathbb{T},\mathbb{U}]$ 称为是*正规的*, 如果 $\deg(I,\mathrm{lv}(T))=0$ 对任意 $T\in\mathbb{T}$ 和 $I\in\mathrm{ini}(\mathbb{T}\cup\mathbb{U})$ 成立.

三角列 $\mathbb{T}$ 称为是*正规的*, 如果 $[\mathbb{T},\mathrm{ini}(\mathbb{I})]$ 是正规的.

换言之, 正规三角系统 $[\mathbb{T},\mathbb{U}]$ 中任意多项式的初式都不含有 $\mathbb{T}$ 的依量. 在文献 [25] 中, 正规三角列被称为 p 链. 在 $\mathbb{T}$ 正规时, 对 $[\mathbb{T},\mathrm{ini}(\mathbb{I})]$ 投影颇为平凡 (见 4.1 节). 下述算法展示如何从任意简单列求得正规简单列.

算法 Norm: $[\mathbb{T}^*,\mathbb{F}]\leftarrow\mathrm{Norm}(\mathbb{T})$. 任给简单列 $\mathbb{T}\subset\mathcal{K}[\boldsymbol{x}]$, 本算法计算正规简单列 $\mathbb{T}^*$ 与多项式组 $\mathbb{F}$, 使得

$$\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}})=\mathrm{Zero}(\mathbb{T}^*/\tilde{\mathbb{T}}\cup\mathbb{F})\cup\bigcup_{F\in\mathbb{F}}\mathrm{Zero}(\mathbb{T}\cup\{F\}/\tilde{\mathbb{T}}),$$

且 $\deg(F,\mathrm{lv}(T))=0$ 对任意 $F\in\mathbb{F}$ 和 $T\in\mathbb{T}$ 成立, 这里 $\tilde{\mathbb{T}}$ 或者为 $\emptyset$, 或者是任一使得 $[\mathbb{T},\tilde{\mathbb{T}}]$ 为简单系统的三角列.

N1. 设 $\mathbb{T}$ 中的多项式依次为 $T_1,\cdots,T_r$, 且命 $\mathbb{F}\leftarrow\emptyset$.

N2. 对 $i=r,\cdots,2$ 执行下列步骤:

N2.1. 计算

$$R \leftarrow \operatorname{res}(\operatorname{ini}(T_i),[T_1,\cdots,T_{i-1}])$$

与多项式 Q, 使得

$$Q_1T_1+\cdots+Q_{i-1}T_{i-1}+Q\cdot\operatorname{ini}(T_i)=R$$

对某些 $Q_1,\cdots,Q_{i-1}\in\mathcal{K}[\boldsymbol{x}]$ 成立.

N2.2. 计算

$$T_i^* \leftarrow R\cdot\operatorname{lv}(T_i)^{\operatorname{ldeg}(T_i)}+Q\cdot\operatorname{red}(T_i).$$

如果 $R\notin\mathcal{K}$, 并且 $\operatorname{sqfr}(R)\nmid\prod_{F\in\operatorname{ini}(\mathbb{T})\cup\mathbb{F}}F$, 则命 $\mathbb{F}\leftarrow\mathbb{F}\cup\{R\}$.

N3. 命 $\mathbb{T}^*\leftarrow[T_1,T_2^*,\cdots,T_r^*]$.

证 只需证明正确性. 设 $\mathbb{T}=[T_1,\cdots,T_r]$, 且

$$p_i=\operatorname{cls}(T_i),\ I_i=\operatorname{ini}(T_i),\ d_i=\operatorname{ldeg}(T_i),\quad 1\le i\le r,$$

而

$$R_i=\operatorname{res}(I_i,[T_1,\cdots,T_{i-1}]),\quad 2\le i\le r.$$

由于 $\mathbb{T}$ 是简单列, 依推论 3.2.7 每个 R_i 都是不含有变元 $x_{p_1},\cdots,x_{p_{i-1}}$ 的非零多项式. 换言之, 对任意 i 和 j 有 $\deg(R_i,x_{p_j})=0$. 由引理 3.2.5, 存在多项式 Q_{ij} 与 Q_i, 使得

$$\sum_{j=1}^{i-1}Q_{ij}T_j+Q_iI_i=R_i,\quad 2\le i\le r. \tag{5.1.1}$$

令

$$\begin{aligned}T_i^* &= R_ix_{p_i}^{d_i}+Q_i\cdot\operatorname{red}(T_i),\quad 2\le i\le r,\\ \mathbb{T}^* &= [T_1,T_2^*,\cdots,T_r^*],\quad \mathbb{F}=\{R_2,\cdots,R_r\}.\end{aligned}$$

如果 $R_i\in\mathcal{K}$ 或者 R_i 的每个不可约因子都整除 $\operatorname{ini}(\mathbb{T})$ 中的某个多项式或另一 R_j $(j\ne i)$, 那么 R_i 是不必要的, 因而可从 $\mathbb{F}$ 中删除. 设 $\tilde{\mathbb{T}}$ 或为 $\emptyset$, 或为使得 $[\mathbb{T},\tilde{\mathbb{T}}]$ 构成简单系统的任一三角列. 今欲证

$$\operatorname{Zero}(\mathbb{T}/\tilde{\mathbb{T}})=\operatorname{Zero}(\mathbb{T}^*/\tilde{\mathbb{T}}\cup\mathbb{F})\cup\bigcup_{i=2}^{r}\operatorname{Zero}(\mathbb{T}\cup\{R_i\}/\tilde{\mathbb{T}}). \tag{5.1.2}$$

为此考虑任意 i, 且设

$$\bar{\boldsymbol{x}}_{p_i-1} \in \mathrm{Zero}([T_1,\cdots,T_{i-1}]/\tilde{\mathbb{T}}^{(p_i-1)} \cup \mathbb{F}).$$

由 (5.1.1) 知

$$Q_i(\bar{\boldsymbol{x}}_{p_i-1})I_i(\bar{\boldsymbol{x}}_{p_i-1}) = R_i(\bar{\boldsymbol{x}}_{p_i-1}) \neq 0.$$

所以在 $\bar{\boldsymbol{x}}_{p_i-1}$ 替代 $\boldsymbol{x}_{p_i-1}$ 之后,

$$T_i^* = Q_iT_i = R_ix_{p_i}^{d_i} + Q_i \cdot \mathrm{red}(T_i)$$

与 T_i 关于 x_{p_i} 具有相同的 d_i 个互异零点 (因而前者无平方因子). 由此即得

$$\mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}} \cup \mathbb{F}) = \mathrm{Zero}(\mathbb{T}^*/\tilde{\mathbb{T}} \cup \mathbb{F}),$$

于是零点关系 (5.1.2) 成立.

显然, $\mathbb{T}^*$ 是正规的 (但 $[\mathbb{T}^*, \tilde{\mathbb{T}} \cup \mathbb{F}]$ 并不一定是简单系统). 剩下的是要证明 $\mathbb{T}^*$ 为简单列. 事实上, 我们可以从 $\tilde{\mathbb{T}} \cup \mathbb{F}$ 构造出三角列或空集 $\tilde{\mathbb{T}}^*$, 使得 $[\mathbb{T}^*, \tilde{\mathbb{T}}^*]$ 为简单系统. 构造过程如下. 置 $R = R_2 \cdots R_r$. 我们重复下列步骤直至 $R \in \mathcal{K}$:

1. 若存在 $T \in \tilde{\mathbb{T}}$, 使得 $\mathrm{cls}(T) = \mathrm{cls}(R)$, 则命 $R \leftarrow RT$, $\tilde{\mathbb{T}} \leftarrow \tilde{\mathbb{T}} \setminus \{T\}$.

2. 计算 $\tilde{R} \leftarrow \mathrm{sqfr}(R)$, 且命

$$\tilde{\mathbb{T}} \leftarrow \tilde{\mathbb{T}} \cup \{\tilde{R}\}, \quad R \leftarrow \mathrm{ini}(\tilde{R}) \cdot \mathrm{res}\left(\tilde{R}, \frac{\partial \tilde{R}}{\partial \mathrm{lv}(\tilde{R})}, \mathrm{lv}(\tilde{R})\right).$$

设 $\tilde{\mathbb{T}}^*$ 为最后的 $\tilde{\mathbb{T}}$; 若非空, 则将其排为三角列, 那么不难按定义验证 $[\mathbb{T}^*, \tilde{\mathbb{T}}^*]$ 为简单系统 (类似的验证见于命题 4.5.7 的证明). 所以 $\mathbb{T}^*$ 是正规简单列. □

引理 5.1.1 从任意正规简单列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$, 可以求得正规、约化且本原的简单列 $\mathbb{T}^*$, 使得

$$\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})) = \mathrm{Zero}(\mathbb{T}^*/\mathrm{ini}(\mathbb{T})).$$

证 设 $\mathbb{T} = [T_1, \cdots, T_r]$, 且命

$$T_i^* = \mathrm{pp}(\mathrm{prem}(T_i, \mathbb{T}^{\{i-1\}}), \mathrm{lv}(T_i)), \quad 2 \leq i \leq r.$$

因为 $\mathbb{T}$ 正规, 所以 T_i^* 是适当定义的且是本原的, 并有 $\mathrm{cls}(T_i^*) = \mathrm{cls}(T_i)$. 命

$$\mathbb{T}^* = [T_1, T_2^*, \cdots, T_r^*],$$

那么 $\mathbb{T}^*$ 是约化的, 也是本原的. 引理中 $\mathbb{T}^*$ 与 $\mathbb{T}$ 之间的零点关系容易验证.

□

注 5.1.1 由算法 Norm 从简单列 $\mathbb{T}$ 求得的正规简单列 $\mathbb{T}^*$ 和多项式组 $\mathbb{F}$ 具有以下性质：对任意多项式 G 和使 $[\mathbb{T},\tilde{\mathbb{T}}]$ 为简单系统的三角列或空集 $\tilde{\mathbb{T}}$ 有

$$\mathrm{Zero}(\mathbb{T}^*/\tilde{\mathbb{T}}\cup\mathbb{F})\subset\mathrm{Zero}(G)\iff\mathrm{prem}(G,\mathbb{T})=0.$$

按照引理 5.1.1, 该性质在 $\mathbb{T}^*$ 约化和本原时仍然成立. 其证明与定理 3.4.4 的证明类似；只需注意 $\mathbb{F}$ 的所有多项式都不含有 $\mathbb{T}^*$ 的依量.

实际上，算法 Norm 对任意正则列 $\mathbb{T}$ 都适用；此时任意 $I\in\mathrm{ini}(\mathbb{T})$ 对 $\mathbb{T}$ 的结式 R 都不恒为零. 我们也可以尝试将任意三角列 $\mathbb{T}$ 正规化，但不能保证一定成功. 以下算法便是为此而设计的，它在成功时输出正规化的三角列. 该算法在 $\mathbb{T}$ 正则、简单或不可约时总会成功.

算法 NormG: $[\mathbb{T}^*,\mathbb{F}]\leftarrow\mathrm{NormG}(\mathbb{T})$. 任给三角列 $\mathbb{T}\subset\mathcal{K}[\boldsymbol{x}]$, 本算法计算 $[\mathbb{T}^*,\mathbb{F}]$, 使得或者 $\mathbb{T}^*=\mathtt{Fail}$ (这时算法失败), 或者 $\mathbb{T}^*$ 为正规三角列，而 $\mathbb{F}$ 为多项式组，满足

$$\mathrm{Zero}(\mathbb{T}/\mathbb{F})\subset\mathrm{Zero}(\mathbb{T}^*),\quad\mathrm{Zero}(\mathbb{T}^*/\mathrm{ini}(\mathbb{T}^*))\subset\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})).\tag{5.1.3}$$

N1. 设 $\mathbb{T}$ 中的多项式依次为 $T_1,\cdots,T_r$, 且命 $\mathbb{F}\leftarrow\emptyset,T_r^*\leftarrow T_r$. 若 $r=1$, 则命 $\mathbb{T}^*\leftarrow[T_1^*]$, 且算法终止.

N2. 对 $i=r-1,\cdots,1$ 执行下列步骤：

N2.1. 命 $I\leftarrow\mathrm{ini}(T_r^*)$. 若 $\mathrm{cls}(I)<\mathrm{cls}(T_i)$, 则转至 N3; 否则命 $y\leftarrow\mathrm{lv}(T_i)$.

N2.2. 计算 $R\leftarrow\gcd(T_i,I,y)$ 与多项式 Q, 使得 $R=PT_i+QI$ 对某一 $P\in\mathcal{K}[\boldsymbol{x}]$ 成立.

N2.3. 若 $\mathrm{cls}(R)<\mathrm{cls}(T_i)$, 则转至 N2.4. 否则，计算

$$D\leftarrow\mathrm{Remo}\left(\frac{T_i}{R},R,y\right),$$

且命 $\mathbb{F}\leftarrow\mathbb{F}\cup\{R\}$. 若 $\mathrm{cls}(D)=\mathrm{cls}(T_i)$, 则命 $T_i\leftarrow D$; 否则命 $\mathbb{T}^*\leftarrow\mathtt{Fail}$, 且算法终止.

N2.4. 命 $T_r^*\leftarrow R\cdot\mathrm{lv}(T_r^*)^{\mathrm{ldeg}(T_r^*)}+Q\cdot\mathrm{red}(T_r^*)$.

N3. 计算

$$[\mathbb{T}^\star,\mathbb{F}^\star]\leftarrow\mathrm{NormG}([T_1,\cdots,T_{r-1}]).$$

若 $\mathbb{T}^\star=\mathtt{Fail}$, 则命 $\mathbb{T}^*\leftarrow\mathtt{Fail}$; 否则命

$$\mathbb{F}\leftarrow\mathbb{F}\cup\mathbb{F}^\star,\quad\mathbb{T}^*\leftarrow\mathbb{T}^\star\cup[T_r^*].$$

NormG 中的子算法 Remo 如下.

算法 Remo: $H \leftarrow \mathrm{Remo}(F, G, x_k)$. 给定 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式 F 和 G 以及变元 x_k, 本算法计算多项式 H, 使得 $\gcd(H, G, x_k)$ 不含有 x_k.

命 $R \leftarrow \gcd(F, G, x_k)$.

若 $\deg(R, x_k) = 0$, 则命 $H \leftarrow F$; 否则, 计算 $H \leftarrow \mathrm{Remo}(F/R, G, x_k)$.

证　NormG 的终止性很明显, 所以我们只需证明它的正确性. 与算法中的记号一致, 设 $|\mathbb{T}| = r$, 那么 $r = 1$ 为平凡情形.

对 $r > 1$, 假定步骤 N2 已对 $i = r-1, \cdots, k+1$ 执行过, 并用 $\tilde{\mathbb{F}}$ 和

$$\tilde{\mathbb{T}} = [T_1(\boldsymbol{z}_1), \cdots, T_{r-1}(\boldsymbol{z}_{r-1}), T_r^*(\boldsymbol{z}_r)]$$

分别表示 $\mathbb{F}$ 和 $\mathbb{T}$ 的当前值; 和通常一样这里 $\boldsymbol{z}_i$ 代表 $(\boldsymbol{u}, y_1, \cdots, y_i)$, 而 $\boldsymbol{z} = \boldsymbol{z}_r$, 那么在用 $\tilde{\mathbb{F}}$ 和 $\tilde{\mathbb{T}}$ 分别替换 $\mathbb{F}$ 和 $\mathbb{T}^*$ 之后 (5.1.3) 式成立.

现对 $i = k$ 考虑 N2. 置 $I_j = \mathrm{ini}(T_j)$, $1 \le j \le r-1$, 而 $I = \mathrm{ini}(T_r^*)$, 那么 $I \in \mathcal{K}[\boldsymbol{z}_k]$. 若 $\mathrm{cls}(I) < \mathrm{cls}(T_k)$, 则对下一重复 $i = k-1$ 进行. 否则的话, 假设 $\mathrm{cls}(I) = \mathrm{cls}(T_k)$. 这时有两种情形:

情形 1. T_k 和 I 关于 $y_k = \mathrm{lv}(T_k)$ 互素, 即 $R = \gcd(T_k, I, y_k) \in \mathcal{K}[\boldsymbol{z}_{k-1}]$. 这与 Norm 所处理的情形类似. 我们可以确定多项式 P, $Q \in \mathcal{K}[\boldsymbol{z}_k]$, 使得

$$PT_k + QI = R \in \mathcal{K}[\boldsymbol{z}_{k-1}]. \tag{5.1.4}$$

将 T_r^* 写成 $T_r^* = Iy_r^d + \mathrm{red}(T_r^*)$ 并将 (5.1.4) 式的两边乘上 y_r^d 可得

$$QT_r^* = Ry_r^d + Q \cdot \mathrm{red}(T_r^*) - PT_k y_r^d, \tag{5.1.5}$$

式中 $d = \mathrm{ldeg}(T_r^*)$. 命

$$\hat{T}_r = Ry_r^d + Q \cdot \mathrm{red}(T_r^*).$$

明显有 $\mathrm{lv}(\hat{T}_r) = \mathrm{lv}(T_r^*) = y_r$. 由此可知 $\hat{\mathbb{T}} = [T_1, \cdots, T_{r-1}, \hat{T}_r]$ 为三角列. 现欲证

$$\mathrm{Zero}(\tilde{\mathbb{T}}) \subset \mathrm{Zero}(\hat{\mathbb{T}}), \quad \mathrm{Zero}(\hat{\mathbb{T}}/\mathrm{ini}(\hat{\mathbb{T}})) \subset \mathrm{Zero}(\tilde{\mathbb{T}}/\mathrm{ini}(\tilde{\mathbb{T}})).$$

由于 $\hat{T}_r$ 可以写成 T_k 和 T_r^* 的线性组合, 其系数为多项式, 所以第一个关系显而易见. 注意 $\mathrm{ini}(\hat{T}_r) = R$. 因此对任意 $\bar{\boldsymbol{z}} \in \mathrm{Zero}(\hat{\mathbb{T}}/\mathrm{ini}(\hat{\mathbb{T}}))$ 都有

$$\begin{aligned} &T_j(\bar{\boldsymbol{z}}) = 0, \ I_j(\bar{\boldsymbol{z}}) \ne 0, \quad 1 \le j \le r-1, \\ &I(\bar{\boldsymbol{z}}) \ne 0, \quad R(\bar{\boldsymbol{z}}) \ne 0. \end{aligned}$$

从 (5.1.5) 以及 $\hat{T}_r$ 的确定可以看出 $Q(\bar{z})T_r^*(\bar{z})=0$. 另一方面, 由 (5.1.4) 知 $Q(\bar{z})I(\bar{z})\neq 0$. 因此有

$$T_r^*(\bar{z})=0,\quad I(\bar{z})\neq 0.$$

所以 $\bar{z}\in \mathrm{Zero}(\tilde{\mathbb{T}}/\mathrm{ini}(\tilde{\mathbb{T}}))$; 第二个零点关系获证.

情形 2. T_k 和 I 关于 y_k 不是互素的. 这时, 它们有导元为 y_k 的公因子. 现将 R (即 T_k 和 I 关于 y_k 的最大公因子) 所有可能的因子都从 T_k 中抹去 (如子算法 Remo 所为), 并用 D 表示所得的多项式. 若 $\mathrm{cls}(D)<\mathrm{cls}(T_k)$, 则算法终止, 并以 $\mathbb{T}^*=\mathbf{Fail}$ 为输出. 否则,

$$\mathbb{T}'=[T_1,\cdots,T_{k-1},D,T_{k+1},\cdots,T_{r-1},T_r^*]$$

为三角列. 因此有

$$\mathrm{Zero}(\tilde{\mathbb{T}}/R)\subset \mathrm{Zero}(\mathbb{T}'),\quad \mathrm{Zero}(\tilde{\mathbb{T}}/\mathrm{ini}(\tilde{\mathbb{T}}))=\mathrm{Zero}(\mathbb{T}'/\mathrm{ini}(\mathbb{T}')).$$

由于现在 D 和 I 关于 y_k 互素, 因而可视 $\mathbb{T}'$ 为 $\tilde{\mathbb{T}}$, 将问题化为情形 1. 于是可以确定 $\hat{\mathbb{T}}$ 和 $\hat{\mathbb{F}}$, 使得

$$\begin{aligned}&\mathrm{Zero}(\tilde{\mathbb{T}}/\hat{\mathbb{F}})\subset \mathrm{Zero}(\mathbb{T}')\subset \mathrm{Zero}(\hat{\mathbb{T}}),\\&\mathrm{Zero}(\hat{\mathbb{T}}/\mathrm{ini}(\hat{\mathbb{T}}))\subset \mathrm{Zero}(\mathbb{T}'/\mathrm{ini}(\mathbb{T}'))=\mathrm{Zero}(\tilde{\mathbb{T}}/\mathrm{ini}(\tilde{\mathbb{T}})).\end{aligned}$$

总之, 在任一情形重复步骤 N2 或者失败, 以 $\mathbb{T}^*=\mathbf{Fail}$ 为输出, 或者生成三角列 $\mathbb{T}=\mathbb{T}_r,\cdots,\mathbb{T}_1$ 与多项式组 $\mathbb{F}_{r-1},\cdots,\mathbb{F}_1$ 满足

$$\begin{aligned}&\mathrm{Zero}(\mathbb{T}_r/\mathbb{F}_{r-1})\subset \mathrm{Zero}(\mathbb{T}_{r-1}),\cdots,\mathrm{Zero}(\mathbb{T}_2/\mathbb{F}_1)\subset \mathrm{Zero}(\mathbb{T}_1),\\&\mathrm{Zero}(\mathbb{T}_1/\mathrm{ini}(\mathbb{T}_1))\subset\cdots\subset \mathrm{Zero}(\mathbb{T}_{r-1}/\mathrm{ini}(\mathbb{T}_{r-1}))\subset \mathrm{Zero}(\mathbb{T}_r/\mathrm{ini}(\mathbb{T}_r)).\end{aligned}$$

置 $\bar{\mathbb{F}}=\mathbb{F}_{r-1}\cup\cdots\cup\mathbb{F}_1$, 我们有

$$\begin{aligned}&\mathrm{Zero}(\mathbb{T}/\bar{\mathbb{F}})=\mathrm{Zero}(\mathbb{T}_r/\bar{\mathbb{F}})\subset \mathrm{Zero}(\mathbb{T}_1),\\&\mathrm{Zero}(\mathbb{T}_1/\mathrm{ini}(\mathbb{T}_1))\subset \mathrm{Zero}(\mathbb{T}_r/\mathrm{ini}(\mathbb{T}_r))=\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})).\end{aligned}$$

设

$$\mathbb{T}_1=[T_1',\cdots,T_r'],\quad \mathbb{T}_1'=[T_1',\cdots,T_{r-1}'].$$

注意 $\mathrm{ini}(T_r')\in\mathcal{K}[\boldsymbol{u}]$. 因 $\mathbb{T}_1'$ 含有 $r-1$ 个多项式, 故在不失败时可依据归纳法计算良好正规三角列 $\mathbb{T}^*$ 与多项式组 $\mathbb{F}^*$ (如步骤 N3 所示), 使得

$$\mathrm{Zero}(\mathbb{T}_1'/\mathbb{F}^*)\subset \mathrm{Zero}(\mathbb{T}^*),\quad \mathrm{Zero}(\mathbb{T}^*/\mathrm{ini}(\mathbb{T}^*))\subset \mathrm{Zero}(\mathbb{T}_1'/\mathrm{ini}(\mathbb{T}_1')).$$

今置 $\mathbb{T}^* = \mathbb{T}^* \cup [T_r']$, $\mathbb{F} = \bar{\mathbb{F}} \cup \mathbb{F}^*$, 那么 (5.1.3) 中的零点关系成立. 现如所欲求, $\mathbb{T}^*$ 中所有多项式的初式皆属于 $\mathcal{K}[\boldsymbol{u}]$; 因而它们对 $\mathbb{T}^*$ 都是约化的. 换言之, $\mathbb{T}^*$ 是良好正规三角列, 于是算法的正确性获证. □

注 5.1.2　对于从任一三角列 $\mathbb{T}$ 用 Norm 或 NormG 求得的正规三角列 $\mathbb{T}^*$, 无法保证

$$\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})) = \mathrm{Zero}(\mathbb{T}^*/\mathrm{ini}(\mathbb{T}^*)),$$

即便 $\mathbb{T}$ 是简单列. 这也是为何 Norm 需要计算附加多项式组 $\mathbb{F}$. 作为例子, 考虑

$$\mathbb{T} = [x_2^2 + x_1, (x_3 - x_2)\, x_4 + 1].$$

关于 $x_1 \prec \cdots \prec x_4$, $\mathfrak{S} = [\mathbb{T}, [x_1, x_3 - x_2]]$ 为简单系统, 因而 $\mathbb{T}$ 是简单列. $\mathbb{T}$ 也是不可约的. 其正规化给出

$$\mathbb{T}^* = [x_2^2 + x_1, (x_3^2 + x_1)\, x_4 + x_3 + x_2].$$

现有

$$\begin{aligned}\mathrm{Zero}(\mathbb{T}/\mathrm{ini}(\mathbb{T})) &= \mathrm{Zero}(\mathbb{T}/(x_3 - x_2)) \\ &\neq \mathrm{Zero}(\mathbb{T}^*/(x_3^2 + x_1)) = \mathrm{Zero}(\mathbb{T}^*/\mathrm{ini}(\mathbb{T}^*)).\end{aligned}$$

这可以通过验证

$$\left(-1, 1, -1, \frac{1}{2}\right) \in \mathrm{Zero}(\mathbb{T}/(x_3 - x_2)), \quad \text{但} \quad \notin \mathrm{Zero}(\mathbb{T}^*/(x_3^2 + x_1))$$

而看出. 事实上, $\mathbb{T}$ 可以分解为两个正规简单列 $\mathbb{T}^*$ 和

$$\mathbb{T}' = [x_2^2 + x_1, x_3 + x_2, 2\, x_1 x_4 + x_2],$$

使得

$$\mathrm{Zero}(\mathbb{T}/(x_3 - x_2)) = \mathrm{Zero}(\mathbb{T}^*/(x_3^2 + x_1)) \cup \mathrm{Zero}(\mathbb{T}'/x_1).$$

并且也能从 $\mathfrak{S}$ 求得正规简单系统 $\mathfrak{S}^*$, 使得 $\mathrm{Zero}(\mathfrak{S}) = \mathrm{Zero}(\mathfrak{S}^*)$. $\mathfrak{S}$ 可分解为两个正规简单系统

$$\mathfrak{S}^* = [\mathbb{T}^*, [x_1, x_3^2 + x_1]], \quad \mathfrak{S}' = [\mathbb{T}', [x_1]],$$

使得

$$\mathrm{Zero}(\mathfrak{S}) = \mathrm{Zero}(\mathfrak{S}^*) \cup \mathrm{Zero}(\mathfrak{S}').$$

然而, 若 $\mathbb{T}$ 正则、简单或不可约, 那么 $\mathbb{T}$ 与 $\mathbb{T}^*$ 的正则或一般零点集必定相同. 该结论可用 Norm N2.1 中计算的结式 R 在 $\mathbb{T}$ 的任意正则零点处都不为零这一事实来予以证明.

多项式 P 是 *首一的*, 如果 $\mathrm{lc}(P)=1$. 多项式组 $\mathbb{P}$ 称为是 *首一的*, 如果每个 $P\in\mathbb{P}$ 都是首一的.

定义 5.1.2 三角列 $\mathbb{T}\subset\mathcal{K}[\boldsymbol{x}]$ 称为是 *典范的*, 如果它是正规的、简单的、约化的、本原的, 并且首一的.

这里典范三角列的定义与拉扎尔在文献 [49] 中所给的三角列的定义相似, 但前者比后者稍强. 例如, 对变元序 $x_1\prec x_2\prec x_3$, 按拉扎尔的定义

$$[x_1^2-1,(x_2-x_1)x_3+1]$$

是三角列, 但依定义 5.1.2 它不是典范的.

现在考虑任意多项式组 $\mathbb{P}$. 我们知道如何用算法 SimSer 从 $\mathbb{P}$ 求得简单系统 $[\mathbb{T}_1,\tilde{\mathbb{T}}_1],\cdots,[\mathbb{T}_t,\tilde{\mathbb{T}}_t]$, 使得

$$\mathrm{Zero}(\mathbb{P})=\bigcup_{i=1}^{t}\mathrm{Zero}(\mathbb{T}_i/\tilde{\mathbb{T}}_i).$$

依照算法 Norm 和引理 5.1.1, 我们又能从每个简单列 $\mathbb{T}_i$ 求得约化、正规、本原的简单列 $\mathbb{T}_i^*$ 及多项式组 $\mathbb{F}_i$, 使得

$$\mathrm{Zero}(\mathbb{T}_i/\tilde{\mathbb{T}}_i)=\mathrm{Zero}(\mathbb{T}_i^*/\tilde{\mathbb{T}}_i\cup\mathbb{F})\cup\bigcup_{F\in\mathbb{F}_i}\mathrm{Zero}(\mathbb{T}_i\cup\{F\}/\tilde{\mathbb{T}}_i).$$

将 SimSer 用于每个多项式系统 $[\mathbb{T}_i\cup\{F\},\tilde{\mathbb{T}}_i]$, 我们又可以得到其他约化、正规、本原的简单列和相应的零点分解. 由于每个 $F\in\mathbb{F}_i$ 都不含有 $\mathbb{T}_i$ 的依量, 因而对 $[\mathbb{T}_i\cup\{F\},\tilde{\mathbb{T}}_i]$ 之简单序列中的每个简单系统其第一个三角列应比 $\mathbb{T}$ 含有更多的多项式. 所以上述递归过程必须终止. 最终我们将获得如下形式的零点分解:

$$\mathrm{Zero}(\mathbb{P})=\bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{T}_i/\tilde{\mathbb{T}}_i),\tag{5.1.6}$$

式中每个三角列 $\mathbb{T}_i$ 都是正规、简单、约化和本原的. 按照注 5.1.1, 对任意 $P\in\mathbb{P}$ 有 $\mathrm{prem}(P,\mathbb{T}_i)=0$. 类似于证明定理 3.4.6 的简单推理表明 (5.1.6) 中的每个 $\tilde{\mathbb{T}}_i$ 都可以用 $\mathrm{ini}(\mathbb{T}_i)$ 来替换. 对每个 $T\in\mathbb{T}_i$, 将 T 化为首一是不足道的: 用 $\mathrm{lc}(T)$ 除 T 即可. 于是下述定理得以建立.

定理 5.1.2 有一算法, 它可以从任意多项式组 $\mathbb{P}\subset\mathcal{K}[\boldsymbol{x}]$ 求得有限多个典范三角列 $\mathbb{T}_1,\cdots,\mathbb{T}_e$, 使得

$$\mathrm{Zero}(\mathbb{P})=\bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{T}_i/\mathrm{ini}(\mathbb{T}_i)).$$

上面的零点分解不一定是*极小的*. 可用推论 3.4.5 将某些多余的零点集抹去.

例 5.1.1 参见例 2.4.1 中的多项式组 $\mathbb{P}$ 及其在例 3.3.4 中的简单序列. 简单列 $\mathbb{T}_i$ 仅在 $i=2,4,5$ 时是正规的, 而对其他 i 都不是. 我们首先考虑 $\mathbb{T}_1=[T_1,T_2,T_3]$, 其中

$$\begin{aligned}T_1&=z^3-z^2+r^2-1,\\T_2&=x^4+z^2x^2-r^2x^2+z^4-2z^2+1,\\T_3&=xy+z^2-1.\end{aligned}$$

易见 $\mathrm{ini}(T_1)=\mathrm{ini}(T_2)=1$, 而 $\mathrm{ini}(T_3)=x$. 也容易验证

$$R=\mathrm{res}(x,[T_1,T_2])=(r^2-1)^2(r^2-3)^2=xQ+Q_1T_1+Q_2T_2,$$

其中

$$Q=-x(x^2+z^2-r^2)(r^4z^2-2r^2z^2+2z^2-2r^4z+3r^2z-z+3r^4-7r^2+4).$$

R 的所有不可约因子都整除 $\tilde{\mathbb{T}}_1$ 中仅有的多项式 (见例 3.3.4), 所以 R 是不必要的. 因此 $\mathrm{Norm}(\mathbb{T}_1)$ 的输出 $\mathbb{F}$ 是空集, 而 $\mathbb{T}_1$ 则正规化为 $\mathbb{T}_1^*=[T_1,T_2,T_3^*]$, 使得

$$\mathrm{Zero}(\mathbb{T}_1/\tilde{\mathbb{T}}_1)=\mathrm{Zero}(\mathbb{T}_1^*/\mathbb{U}_1),$$

其中 $T_3^*=Ry+Q(z^2-1)$. 用 T_2 和 T_1 约化 T_3^* 并取其伪余式的本原部分, 我们有

$$\begin{aligned}\hat{T}_3&=\mathrm{pp}(\mathrm{prem}(T_3^*,[T_1,T_2]),y)\\&=(r^4-4r^2+3)y-z^2x^3+r^2zx^3-zx^3-r^2x^3+x^3+r^2z^2x\\&\quad-z^2x-r^4zx+2r^2zx-zx+2r^2x-2x.\end{aligned}$$

$\hat{T}_3$ 是首一的, 因而 $\hat{\mathbb{T}}_1=[T_1,T_2,\hat{T}_3]$ 为典范三角列.

对其他非正规简单列, 相应的结式 R_i 都是常数. 这是因为对 $i>1$ 有 $|\mathbb{T}_i|=4$, 即变元的个数. 因此可从每个 $\mathbb{T}_i$ 得到典范三角列 $\hat{\mathbb{T}}_i$, $i=3,6,\cdots,9$. 这些典范三角列中的多项式之初式都应该是常数. 特别有 $\hat{\mathbb{T}}_i=\mathbb{T}_i$, $i=2,3,5$. 故得

$$\mathrm{Zero}(\mathbb{P})=\mathrm{Zero}\Big(\hat{\mathbb{T}}_1/(r^2-1)(r^2-3)\Big)\cup\bigcup_{i=2}^{9}\mathrm{Zero}(\hat{\mathbb{T}}_i).$$

该分解并不是极小的：对 $i=3,4,6,\cdots,9$, $\mathrm{Zero}(\hat{\mathbb{T}}_i)$ 都可抹去. 换言之，求并指标 i 只需取 2 和 5, 即

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}\Big(\hat{\mathbb{T}}_1/(r^2-1)\,(r^2-3)\Big) \cup \mathrm{Zero}(\mathbb{T}_2) \cup \mathrm{Zero}(\mathbb{T}_5).$$

上例中计算了诸多多余的简单列，将其正规化，并最终将其抹去以便获得典范零点分解. 一个关键的问题是如何避免计算这样的多余简单列或系统. 给出该问题的完整解答并非易事，而实际计算时我们又必须有有效的策略来尽早排除多余分支. 在关注效率时，我们建议计算不可约三角序列而不是简单序列. 由前者获得典范零点分解比由后者更容易. 如前所述，简单序列的意义主要在理论上而不在实用上.

也可将正规化过程并入 SimSer 以及其他分解算法. 此外，结式计算也可由子结式计算来替代；后者已用于若干算法，包括 SimSer 和 RegSer. 实际上，我们可以设计一个算法，它能从任一多项式组计算出一个简单或正则序列，使得其中的简单或正则系统都是正规的. 对每个正规简单或正则系统 $[\mathbb{T},\tilde{\mathbb{T}}]$, 也可以要求每个多项式 $P\in\mathbb{T}\cup\tilde{\mathbb{T}}$ 都不含有 $\mathbb{T}\setminus[P]$ 的依量. 对此我们不再作进一步的讨论.

拉扎尔在 [49] 中提出了另一算法将多项式组分解为典范三角列. 该算法使用域扩张上的增量计算，颇为繁复. 上述文献中有算法的技术性描述，但无正式证明. 后来拉扎尔的学生对其算法作了改进 (参阅 [2]).

5.2 不可约简单系统

简单系统称为是*不可约的*或*素的*，如果它作为三角系统是不可约的. 我们希望将任意多项式系统 $\mathfrak{P}$ 分解为不可约简单系统. 这可以通过先将 $\mathfrak{P}$ 分解为不可约三角系统 $\mathfrak{T}_i$ 再从每个 $\mathfrak{T}_i$ 计算简单系统来实现.

为了详述这一过程，考虑不可约三角系统 $[\mathbb{T},\mathbb{U}]$, 且命

$$\mathbb{U}' = \left\{\frac{\partial T}{\partial \mathrm{lv}(T)}:\ T\in\mathbb{T}\right\},$$

而

$$\mathbb{R} = \{\mathrm{sqfr}(\mathrm{res}(U,\mathbb{T})):\ U\in\mathbb{U}\cup\mathbb{U}'\}.$$

由于 $\mathbb{T}$ 不可约，且对每个 $U\in\mathbb{U}\cup\mathbb{U}'$ 有 $\mathrm{prem}(U,\mathbb{T})\neq 0$, 所以任意多项式 $R\in\mathbb{R}$ 都非零且不含 $\mathbb{T}$ 的依量，并且

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \mathrm{Zero}(\mathbb{T}/\mathbb{R}) \cup \bigcup_{R\in\mathbb{R}} \mathrm{Zero}(\mathbb{T}\cup\{R\}/\mathbb{U}).$$

计算 $[\emptyset, \mathbb{R}]$ 的简单序列 $[\mathbb{T}_1, \tilde{\mathbb{T}}_1], \cdots, [\mathbb{T}_q, \tilde{\mathbb{T}}_q]$. 必有某个 $\mathbb{T}_i$ 为空集. 若不然, 可假设所有 $\mathbb{T}_i$ 都非空; 又设 y 为一新变元, 那么在 $\mathcal{K}[\boldsymbol{x}, y]$ 中有

$$\bigcup_{i=1}^{q} \mathrm{Zero}(\mathbb{T}_i \cup [y]/\tilde{\mathbb{T}}_i) = \mathrm{Zero}([y]/\mathbb{R}),$$

$$\max_{1 \le i \le q} \dim(\mathbb{T}_i \cup [y]) \le n - 1,$$

且 $\dim([y]) = n$. 这与推论 6.1.6 相矛盾. 所以可假定 $\mathbb{T}_1, \cdots, \mathbb{T}_l$ $(1 \le l \le q)$ 是所有为空集的那些 $\mathbb{T}_i$. 于是

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{l} \mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}}_i) \cup \bigcup_{i=l+1}^{q} \mathrm{Zero}(\mathbb{T} \cup \mathbb{T}_i/\tilde{\mathbb{T}}_i) \cup \bigcup_{R \in \mathbb{R}} \mathrm{Zero}(\mathbb{T} \cup \{R\}/\mathbb{U}).$$

特别指出, $\mathbb{T} \cup \mathbb{T}_i$ $(i > l)$ 和 $\mathbb{T} \cup \{R\}$ $(R \in \mathbb{R})$ 都是从 $\mathbb{T}$ 通过添加至少一个不含 $\mathbb{T}$ 的依量的多项式扩大而得.

今欲证 $[\mathbb{T}, \tilde{\mathbb{T}}_i]$ 为不可约简单系统, $1 \le i \le l$. 为此, 考虑固定的 i (≥ 1 而 $\le l$) 和类为 p 的多项式 $T \in \mathbb{T}$. 设

$$\bar{\boldsymbol{x}}_{p-1} \in \mathrm{Zero}(\mathbb{T}^{(p-1)}/\tilde{\mathbb{T}}_i^{(p-1)}),$$

那么对所有 $R \in \mathbb{R}$ 有 $R(\bar{x}_{p-1}, x_p, \cdots, x_n) \ne 0$. 由 $\mathbb{R}$ 的构造可知 $\mathrm{ini}(T)(\bar{\boldsymbol{x}}_{p-1}) \ne 0$, 且关于 x_p,

$$T(\bar{\boldsymbol{x}}_{p-1}, x_p), \quad \frac{\partial T}{\partial x_p}(\bar{\boldsymbol{x}}_{p-1}, x_p)$$

无次数 ≥ 1 的公因子. 因而 $T(\bar{\boldsymbol{x}}_{p-1}, x_p)$ 无平方因子. 注意, $[\emptyset, \tilde{\mathbb{T}}_i]$ 为简单系统, 而 $\tilde{\mathbb{T}}_i$ 中的任意多项式都不含 $\mathbb{T}$ 的依量. 故 $[\mathbb{T}, \tilde{\mathbb{T}}_i]$ 为简单系统.

以上论述可总结为下面的引理. 它的推论之一是命题 4.5.7.

引理 5.2.1 从 $\mathcal{K}[\boldsymbol{x}]$ 中的任意不可约三角系统 $[\mathbb{T}, \mathbb{U}]$, 可求得有限多个三角列或空集 $\tilde{\mathbb{T}}_1, \cdots, \tilde{\mathbb{T}}_l$ 以及多项式系统 $[\mathbb{F}_1, \mathbb{U}_1], \cdots, [\mathbb{F}_m, \mathbb{U}_m]$, 其中 $\mathbb{F}_j \ne \emptyset$, 使得每个 $[\mathbb{T}, \tilde{\mathbb{T}}_i]$ 都是不可约简单系统, $\mathbb{F}_i$ 中的每个多项式都不含 $\mathbb{T}$ 的依量, 且

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{l} \mathrm{Zero}(\mathbb{T}/\tilde{\mathbb{T}}_i) \cup \bigcup_{j=1}^{m} \mathrm{Zero}(\mathbb{T} \cup \mathbb{F}_j/\mathbb{U}_j).$$

现考虑任意多项式系统 $\mathfrak{P}$, 并设 $[\mathbb{T}_1,\mathbb{U}_1],\cdots,[\mathbb{T}_t,\mathbb{U}_t]$ 为 $\mathfrak{P}$ 的不可约三角序列. 对每个 $[\mathbb{T}_i,\mathbb{U}_i]$, 可按引理 5.2.1 确定三角列或空集 $\tilde{\mathbb{T}}_{i1},\cdots,\tilde{\mathbb{T}}_{il_i}$ 以及多项式系统 $[\mathbb{F}_{i1},\mathbb{U}_{i1}],\cdots,[\mathbb{F}_{im_i},\mathbb{U}_{im_i}]$, 其中 $\mathbb{F}_{ik}\neq\emptyset$, 使得

$$\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)=\bigcup_{j=1}^{l_i}\mathrm{Zero}(\mathbb{T}_i/\tilde{\mathbb{T}}_{ij})\cup\bigcup_{k=1}^{m_i}\mathrm{Zero}(\mathbb{T}_i\cup\mathbb{F}_{ik}/\mathbb{U}_{ik}),$$

这里每个 $[\mathbb{T}_i,\tilde{\mathbb{T}}_{ij}]$ 都是简单系统, 且对任意 $F\in\mathbb{F}_{ik}$ 与 $T\in\mathbb{T}_i$ 都有 $\deg(F,\mathrm{lv}(T))=0$.

我们可以将每个多项式系统 $[\mathbb{T}_i\cup\mathbb{F}_{ik},\mathbb{U}_{ik}]$ 再分解为不可约三角系统 $[\mathbb{T}^*_{ij},\mathbb{U}^*_{ij}]$, 并将引理 5.2.1 用于每个所得的 $[\mathbb{T}^*_{ij},\mathbb{U}^*_{ij}]$, 如此等等. 因 $\mathbb{T}$ 不可约且对任意 $F\in\mathbb{F}_{ik}$ 与 $T\in\mathbb{T}_i$ 有 $\deg(F,\mathrm{lv}(T))=0$, 故 $|\mathbb{T}^*_{ij}|>|\mathbb{T}_i|$. 所以上述递归过程必定终止. 最后, $\mathfrak{P}$ 分解为有限多个不可约简单系统. 换言之, 我们有如下定理.

定理 5.2.2 有一算法, 它可以从 $\mathcal{K}[\boldsymbol{x}]$ 中的任给多项式系统 $\mathfrak{P}$ 求得有限多个不可约简单系统 $\mathfrak{S}_1,\cdots,\mathfrak{S}_e$, 使得

$$\mathrm{Zero}(\mathfrak{P})=\bigcup_{i=1}^{e}\mathrm{Zero}(\mathfrak{S}_i).$$

上述理论性方法的实际应用可能很不理想. 我们如此给出主要是为了简便和易于证明终止性. 对于实际应用, 可以先直接计算每个不可约三角系统 $[\mathbb{T}_i,\mathbb{U}_i]$ 的简单序列, 然后再检验哪些所得的简单系统已不可约. 对可约的简单系统, 可进一步将其分解为不可约三角系统, 并如此继续. 按这种方式, $\mathfrak{P}$ 也能分解为不可约简单系统, 但程序的终止性不甚明显.

例 5.2.1 考虑 (4.4.8) 中的不可约三角系统. 由于 $\dim(\mathbb{T}_2)=\dim(\mathbb{T}_{3j})=0$ $(1\leq j\leq 8)$, 易见, 对 $i=2,31,\cdots,38$, $[\mathbb{T}_i,\emptyset]$ 皆为简单系统. 今重温三角列

$$\mathbb{T}_1=\begin{bmatrix}-z^5+t^4,\\ z^6y^2+2\,t^3z^3y-t^7z^5+2\,t^4z^5-tz^5+t^6,\\ (t^3-1)\,z^3x-z^3y-t^3\end{bmatrix},$$

这里 $t\prec z\prec y\prec x$. 所需考虑的三个多项式的初式和导数的因子为

$$t^3-1,\quad z,\quad z^3y+t^3.$$

由于

$$\mathrm{sqfr}(\mathrm{res}(z,\mathbb{T}_1))=t,\quad \mathrm{sqfr}(\mathrm{res}(z^3y+t^3,\mathbb{T}_1))=t\,(t^3-1),$$

故可取 $\mathbb{R}=\{t,t^3-1\}$. $[\emptyset,\mathbb{R}]$ 的简单序列由单个简单系统 $[\emptyset,\tilde{\mathbb{T}}_1]$ 构成，其中 $\tilde{\mathbb{T}}_1=[t\,(t^3-1)]$. 于是我们获得不可约简单系统 $[\mathbb{T}_1,\tilde{\mathbb{T}}_1]$. 直接计算 $[\mathbb{T}_1,\mathrm{ini}(\mathbb{T}_1)]$ 的简单序列导致同样结果. 无论哪种情形，我们都有

$$\mathrm{Zero}(\mathbb{P})=\mathrm{Zero}(\mathbb{T}_1/\tilde{\mathbb{T}}_1)\cup\mathrm{Zero}(\mathbb{T}_2)\cup\bigcup_{j=1}^{8}\mathrm{Zero}(\mathbb{T}_{3j}).$$

作为分解 $\mathfrak{P}$ 为不可约简单系统的另一途径，我们可以先计算 $\mathfrak{P}$ 的简单序列，再用算法 Decom 将每个所得的简单系统进一步分解为不可约三角系统. 然而，这些三角系统不一定是简单系统，而由其求得简单系统则需用到与上面类似的技巧. 这一方法有明显的缺陷. 由于将多项式化为无平方因子的代价很高，简单序列的计算非常昂贵. 显然，这些花费是无益的，如果所考虑的多项式最终要被分解为不可约因子. 因而我们不再对此进行讨论.

5.3 格罗布讷基

由布赫贝格尔[7]引进的格罗布讷基方法为多项式消元提供了另一高效手段. 该方法已被深入研究，并在下列著作中有详细论述：研究生教材 [3]，大学课本 [21] (第二章) 、 [30] (第一至三章) 和专著 [1] 、 [57] (第二、三章) 等. 因而我们对其不再赘述. 我们将满足于对格罗布讷基方法作一简略介绍，着重点在其消元方面.

对固定的变元序，可以引进不同的 *容许* 项序. 两种常用的容许项序是 *全幂* 和 *纯字典* 序. 就消元而言，我们将使用 1.1 节中介绍的纯字典项序. 下面用到的一些记号也曾在 1.1 节中给出. 本节中所提到的多项式都假定在 $\mathcal{K}[\boldsymbol{x}]$ 中.

布赫贝格尔算法

定义 5.3.1 设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式组，而 G 为任意多项式. 称 G 对 $\mathbb{P}$ 为 *可约的*，如果存在多项式 $P\in\mathbb{P}$ 和项 λ，使得 $\mathrm{coef}(G,\lambda\cdot\mathrm{lt}(P))\neq 0$. 如果没有这样的 P 和 λ 存在，则称 G 对 $\mathbb{P}$ 为 *约化的* 或为 *范式*.

若 G 对 $\mathbb{P}$ 可约，则可求得多项式 $P\in\mathbb{P}$，其中项 $\lambda\cdot\mathrm{lt}(P)$ (关于所用项序) 极大，使得

$$G=b\cdot\lambda\cdot P+H,$$

式中

$$b = \frac{\operatorname{coef}(G, \lambda \cdot \operatorname{lt}(P))}{\operatorname{lc}(P)}.$$

这是 G 到 H 的一步约化，使得 G 的一项被消去．换言之，项 $\lambda \cdot \operatorname{lt}(P)$ 在 H 中不再出现．

若 H 对 $\mathbb{P}$ 可约，则可按同样方式选取 P, b 和 λ 将 H 约化为另一多项式．因约化为诺特关系，这一过程必将终止．也就是说，在有限多步约化之后，所得的多项式 R 对 $\mathbb{P}$ 将是约化的．是时，我们得到如下形式的 *余式公式*:

$$G = \sum_{j=1}^{s} Q_j P_j + R, \tag{5.3.1}$$

其中 $P_j \in \mathbb{P}$, $Q_j, R \in \mathcal{K}[\boldsymbol{x}]$, 而 R 对 $\mathbb{P}$ 是约化的．称多项式 R 为 G 对 $\mathbb{P}$ 的 *余式* 或 *范式*, 记作 $\operatorname{rem}(G, \mathbb{P})$. 又称由 G 求得 R 的过程为 G 对 $\mathbb{P}$ 的 *约化*. 对任意 $\mathbb{Q} \subset \mathcal{K}[\boldsymbol{x}]$, 定义

$$\operatorname{rem}(\mathbb{Q}, \mathbb{P}) \triangleq \{\operatorname{rem}(Q, \mathbb{P}):\ Q \in \mathbb{Q}\}.$$

例 5.3.1 考虑下列多项式:

$$\begin{aligned}
P_1 &= x_1x_4 + x_3 - x_1x_2, \\
P_2 &= 2\,x_4^2 - 2\,x_3x_4 + 5\,x_1x_2x_4 - 5\,x_1x_2x_3, \\
G &= x_1x_4^2 + x_4^2 - x_1x_2x_4 - x_2x_4 + x_1x_2 + 3\,x_2.
\end{aligned}$$

P_1, P_2 和 G 中的单项式已按纯字典序排列．用符号表示，我们有

$$\begin{aligned}
&\operatorname{lt}(P_1) = x_1x_4, \quad \operatorname{lt}(P_2) = x_4^2, \quad \operatorname{lt}(G) = x_1x_4^2; \\
&\operatorname{lc}(P_1) = \operatorname{lc}(G) = 1, \quad \operatorname{lc}(P_2) = 2.
\end{aligned}$$

置 $\mathbb{P} = \{P_1, P_2\}$. G 对 $\mathbb{P}$ 明显可约，譬如

$$G = b \cdot \lambda \cdot \operatorname{lt}(P_1) + H,$$

其中

$$\begin{aligned}
b &= -1, \quad \lambda = x_2, \\
H &= x_1x_4^2 + x_4^2 - x_2x_4 + x_2x_3 - x_1x_2^2 + x_1x_2 + 3\,x_2,
\end{aligned}$$

这时项 $x_1x_2x_4$ 在 H 中不出现．对于上面的约化，消去的项关于项序不是极大．欲选极大项，我们需要先约化 G 中的导单项式 $x_1x_4^2$. 对 $\mathbb{P}$, G 到其余式的约化如下:

$$G = x_4P_2 + H_1, \quad H_1 = \frac{1}{2}P_2 + H_2, \quad H_2 = -\frac{5}{2}P_1 + H_3,$$

其中

$$H_1 = x_4^2 - x_3x_4 - x_2x_4 + x_1x_2 + 3\,x_2,$$
$$H_2 = -\frac{5}{2}\,x_1x_2x_4 - x_2x_4 + \frac{5}{2}\,x_1x_2x_3 + x_1x_2 + 3\,x_2,$$
$$H_3 = -x_2x_4 + \frac{5}{2}\,x_1x_2x_3 + \frac{5}{2}\,x_2x_3 - \frac{5}{2}\,x_1x_2^2 + x_1x_2 + 3\,x_2.$$

现在 H_3 对 $\mathbb{P}$ 已约化，因而不可能有进一步的约化．所以

$$R = \mathrm{rem}(G, \mathbb{P}) = H_3 = G + \frac{5}{2}\,P_1 - \left(x_4 + \frac{1}{2}\right) P_2.$$

一般来说，余式 R 是不唯一的；也就是说，对于 (5.3.1), P_j 从 $\mathbb{P}$ 中的不同选取可以产生不同的余式．那些多项式组 —— 对其每个多项式的所有余式都总是相同 —— 具有特殊意义．

定义 5.3.2　称多项式组 $\mathbb{G} \subset \mathcal{K}[\boldsymbol{x}]$ 为**格罗布讷基**, 如果余式 $\mathrm{rem}(G, \mathbb{G})$ 对所有 $G \in \mathcal{K}[\boldsymbol{x}]$ 都是唯一的．

称 $\mathbb{G}$ 为多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 或理想 $\mathrm{Ideal}(\mathbb{P})$ 的**格罗布讷基**, 如果 $\mathbb{G}$ 为格罗布讷基，且 $\mathrm{Ideal}(\mathbb{P}) = \mathrm{Ideal}(\mathbb{G})$.

定义 5.3.3　$\mathcal{K}[\boldsymbol{x}]$ 中两个非零多项式 F 和 G 的 **S 多项式** 定义为

$$\mathrm{spol}(F, G) \triangleq \mu \cdot F - \frac{\mathrm{lc}(F)}{\mathrm{lc}(G)} \cdot \nu \cdot G,$$

式中 μ 和 ν 是使 $\mathrm{lt}(F) \cdot \mu = \mathrm{lt}(G) \cdot \nu = \mathrm{lcm}(\mathrm{lt}(F), \mathrm{lt}(G))$ 成立的项．

例 5.3.2　对例 5.3.1 中的多项式 P_1 和 P_2，我们有

$$\begin{aligned}\mathrm{spol}(P_1, P_2) &= \mu_1 \cdot P_1 - \frac{\mathrm{lc}(P_1)}{\mathrm{lc}(P_2)} \cdot \mu_2 \cdot P_2 \\ &= x_1x_3x_4 + x_3x_4 - \frac{5}{2}\,x_1^2x_2x_4 - x_1x_2x_4 + \frac{5}{2}\,x_1^2x_2x_3,\end{aligned}$$

其中 $\mu_1 = x_4$, $\mu_2 = x_1$.

定理 5.3.1　多项式组 $\mathbb{G} \subset \mathcal{K}[\boldsymbol{x}]$ 为格罗布讷基当且仅当

$$\mathrm{rem}(\mathrm{spol}(F, G), \mathbb{G}) = 0 \quad \text{对任意 } F, G \in \mathbb{G} \text{ 成立}.$$

该定理指出了格罗布讷基的一个算法特征. 多项式组 $\mathbb{P}$ 是否为格罗布讷基可以通过考虑有限多对 $\mathbb{P}$ 中的多项式来加以检验. 基于定理 5.3.1 我们可将布赫贝格尔[7, 8]算法描述如下.

算法 GroBas: $\mathbb{G} \leftarrow \mathrm{GroBas}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算 $\mathbb{P}$ 的格罗布讷基 $\mathbb{G}$.

G1. 命 $\mathbb{G} \leftarrow \mathbb{P}$, $\Theta \leftarrow \{\{F, G\}\colon\ F \neq G, F, G \in \mathbb{P}\}$.

G2. 重复下列步骤直至 $\Theta = \emptyset$:

G2.1. 设 $\{F, G\}$ 为 Θ 中的元素, 且命 $\Theta \leftarrow \Theta \setminus \{\{F, G\}\}$.

G2.2. 计算 $R \leftarrow \mathrm{rem}\,(\mathrm{spol}(F, G), \mathbb{G})$.

G2.3. 若 $R \neq 0$, 则命

$$\Theta \leftarrow \Theta \cup \{\{R, G\}\colon\ G \in \mathbb{G}\}\,, \quad \mathbb{G} \leftarrow \mathbb{G} \cup \{R\}.$$

上述计算格罗布讷基的算法可图解如下:

$$\begin{array}{cccccccccc} \mathbb{P} = & \mathbb{G}_1 & \subset & \mathbb{G}_2 & \subset & \cdots & \subset & \mathbb{G}_m & = & \mathbb{G} \\ & \Theta_1 & & \Theta_2 & & \cdots & & \Theta_m & & \\ & \mathbb{R}_1 & & \mathbb{R}_2 & & \cdots & & \mathbb{R}_m & = & \emptyset \end{array} \tag{5.3.2}$$

这里

$$\Theta_1 = \{\{F, G\}\colon\ F \neq G, F, G \in \mathbb{P}\},$$

而对 $1 \leq i \leq m - 1$ 有

$$\begin{aligned} \mathbb{R}_i &= \mathrm{rem}(\bar{\Theta}_i, \mathbb{G}_i) \setminus \{0\}, \text{ 对某一 } \bar{\Theta}_i \subset \Theta_i, \text{ 且 } |\mathbb{R}_i| = 1, \\ \Theta_{i+1} &= \Theta_i \setminus \bar{\Theta}_i \cup \{\mathrm{spol}(R, G)\colon\ R \in \mathbb{R}_i, G \in \mathbb{G}_i\}, \\ \mathbb{G}_{i+1} &= \mathbb{G}_i \cup \mathbb{R}_i. \end{aligned}$$

算法在第 m 步终止; 此时 $\mathbb{R}_m = \mathrm{rem}(\Theta_m, \mathbb{G}_m) \setminus \{0\} = \emptyset$.

由定理 5.3.1 可知, 多项式组 $\mathbb{G} = \mathbb{G}_m$ 的确为 $\mathbb{P}$ 的格罗布讷基. 为了说明算法的终止性, 考虑理想序列

$$\mathrm{Ideal}(\mathbb{F}_1) \subset \mathrm{Ideal}(\mathbb{F}_2) \subset \cdots \subset \mathrm{Ideal}(\mathbb{F}_i) \subset \cdots,$$

其中 $\mathbb{F}_i$ 是 $\mathbb{G}_i$ 中多项式的导项构成的集合, 而 $\mathbb{G}_i$ 是从 $\mathbb{P}$ 扩大 i 次所得. 以上序列中理想的关系是真包含, 因而根据 $\mathcal{K}[\boldsymbol{x}]$ 中理想升链的希尔伯特定理该序列必定有限. 有关细节可参阅 [8], [1] (42 和 43 页) 与 [3] (213 至 215 页).

称多项式组 $\mathbb{P}$ 为*约化的*，如果每个多项式 $P \in \mathbb{P}$ 都是首一的，且对 $\mathbb{P}\setminus\{P\}$ 是约化的. 下述算法从任意格罗布讷基求得唯一的*约化格罗布讷基* (见定理 5.3.3).

算法 RedGroBas: $\mathbb{G}^* \leftarrow \text{RedGroBas}(\mathbb{G})$. 给定格罗布讷基 $\mathbb{G} \subset \mathcal{K}[\boldsymbol{x}]$，本算法计算 $\mathbb{G}$ 的约化格罗布讷基 $\mathbb{G}^*$.

R1. 命 $\mathbb{P} \leftarrow \mathbb{G}$, $\mathbb{G}^* \leftarrow \emptyset$.

R2. 重复下列步骤直至 $\mathbb{P} = \emptyset$:

R2.1. 选取多项式 $G \in \mathbb{P}$, 且命 $\mathbb{P} \leftarrow \mathbb{P} \setminus \{G\}$.

R2.2. 若 $\text{lt}(P) \nmid \text{lt}(G)$ 对所有 $P \in \mathbb{P} \cup \mathbb{G}^*$ 成立，则命 $\mathbb{G}^* \leftarrow \mathbb{G}^* \cup \{G\}$.

R3. 重复下列步骤直至 $\mathbb{G}^*$ 约化:

R3.1. 选取对 $\mathbb{G}^* \setminus \{G\}$ 可约的 $G \in \mathbb{G}^*$, 且命 $\mathbb{G}^* \leftarrow \mathbb{G}^* \setminus \{G\}$.

R3.2. 计算 $R \leftarrow \text{rem}(G, \mathbb{G}^*)$. 若 $R \neq 0$, 则命 $\mathbb{G}^* \leftarrow \mathbb{G}^* \cup \{R\}$.

R4. 命 $\mathbb{G}^* \leftarrow \{G/\text{lc}(G) \colon G \in \mathbb{G}^*\}$.

关于该算法的证明，参阅 [3] (203, 204, 216 和 217 页).

例 5.3.3 考虑例 5.3.1 中的多项式. 又设

$$P_3 = x_3x_4 - 2x_2^2 - x_1x_2 - 1.$$

对于 $x_1 \prec \cdots \prec x_4$ 确定的纯字典项序，$\{P_1, G, P_3\}$ 的约化格罗布讷基为

$$\mathbb{G} = \begin{bmatrix} x_1x_2^2 + x_2^2 - x_1x_2 + \dfrac{1}{2}x_1 + \dfrac{1}{2}, \\ x_3^2 - x_1x_2x_3 - 2x_2^2 + x_1^2x_2 + 2x_1x_2 - 1, \\ x_1x_4 + x_3 - x_1x_2, \\ x_2^2x_4 + \dfrac{1}{2}x_4 - x_2^2x_3 + x_2x_3 - \dfrac{1}{2}x_3 - x_2^3 - \dfrac{1}{2}x_2, \\ x_3x_4 - 2x_2^2 - x_1x_2 - 1, \\ x_4^2 - x_2x_4 - 2x_2^2 + 3x_2 - 1 \end{bmatrix}.$$

读者可将该格罗布讷基与例 2.2.3 中的特征列予以比较.

对于同样的变元序和项序，$\{P_1, P_2, P_3\}$ 的格罗布讷基由 9 个多项式构成. 这些多项式相当大，因此没有罗列于此.

我们未对算法 GroBas 予以优化，因而它不太实用．该算法有若干改进版．这些改进算法考虑到优化选取多项式对来构造 S 多项式的准则，附加约化，以及避免生成不必要的 S 多项式．此外，也有学者提出了计算格罗布讷基的替代算法．我们不再介绍这些进展；有兴趣的读者可以阅读前面提到的格罗布讷基理论和方法的有关论著．

性质

格罗布讷基具有良好的特性和结构．不含有常数的格罗布讷基 $\mathbb{G}$ 可以写成如下形式：

$$\mathbb{G}=\begin{bmatrix} G_1(x_1,\cdots,x_{p_1}), \\ \quad\cdots\cdots \\ G_{q_1}(x_1,\cdots,x_{p_1}), \\ G_{q_1+1}(x_1,\cdots,x_{p_1},\cdots,x_{p_2}), \\ \quad\cdots\cdots \\ G_{q_2}(x_1,\cdots,x_{p_1},\cdots,x_{p_2}), \\ \quad\cdots\cdots \\ G_{q_{r-1}+1}(x_1,\cdots,x_{p_1},\cdots,x_{p_2},\cdots,x_{p_r}), \\ \quad\cdots\cdots \\ G_{q_r}(x_1,\cdots,x_{p_1},\cdots,x_{p_2},\cdots,x_{p_r}) \end{bmatrix},$$

这里

$$\begin{aligned} &0<p_1<p_2<\cdots<p_r\le n, \\ &p_i=\operatorname{cls}(G_{q_{i-1}+1})=\cdots=\operatorname{cls}(G_{q_i}), \\ &x_{p_i}=\operatorname{lv}(G_{q_{i-1}+1})=\cdots=\operatorname{lv}(G_{q_i}), \end{aligned}$$

而 $q_0=0$, $q_{i-1}<q_i$ $(1\le i\le r)$．上面的阶梯三角形与 (2.1.1) 形成对照．

以下我们罗列格罗布讷基的若干优良特性．这些性质多与本书的主题——多项式消元——密切相关．有关这些及其他性质的详细介绍，读者可参阅前面提到的著作．

定理 5.3.2 下列性质是等价的：

(a) $\mathbb{G}$ 是 $\mathcal{K}[\boldsymbol{x}]$ 中的格罗布讷基；

(b) 对 $\mathcal{K}[\boldsymbol{x}]$ 中的所有 F 和 G,

$$F-G\in\operatorname{Ideal}(\mathbb{G}) \iff \operatorname{rem}(F,\mathbb{G})=\operatorname{rem}(G,\mathbb{G});$$

(c) 每个非零多项式 $F\in\operatorname{Ideal}(\mathbb{G})$ 对 $\mathbb{G}$ 都是可约的；

(d) 对每个非零多项式 $F \in \mathrm{Ideal}(\mathbb{G})$, 存在多项式 $G \in \mathbb{G}$, 使得 $\mathrm{lt}(G) \mid \mathrm{lt}(F)$;

(e) 对所有 $F \in \mathcal{K}[\boldsymbol{x}]$, $F \in \mathrm{Ideal}(\mathbb{G})$

$$\iff F = \sum_{G \in \mathbb{G}} H_G G, \quad 而 \quad \mathrm{lt}(F) = \max_{G \in \mathbb{G}} \mathrm{lt}(H_G) \cdot \mathrm{lt}(G);$$

(f) $\mathrm{Ideal}(\{\mathrm{lm}(G)\colon\ G \in \mathbb{G}\}) = \mathrm{Ideal}(\{\mathrm{lm}(G)\colon\ G \in \mathrm{Ideal}(\mathbb{G})\})$.

证 见文献 [8] 中定理 6.1, [1] 中 (32 和 33 页) 定理 1.6.2 与 [3] 中 (207 和 208 页) 命题 5.38. □

引进约化格罗布讷基的部分意义在于以下事实: 对任意多项式理想, 其约化格罗布讷基是唯一的. 换言之, 我们有下述定理.

定理 5.3.3 设 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 分别为 $\mathcal{K}[\boldsymbol{x}]$ 中多项式组 $\mathbb{P}_1$ 和 $\mathbb{P}_2$ 的约化格罗布讷基. 若 $\mathrm{Ideal}(\mathbb{P}_1) = \mathrm{Ideal}(\mathbb{P}_2)$, 则 $\mathbb{G}_1 = \mathbb{G}_2$.

证 见 [8] 中定理 6.3, [1] 中 (48 和 49 页) 定理 1.8.7, 或 [3] 中 (209 页) 定理 5.43. □

对任意多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, $\mathrm{GB}(\mathbb{P})$ 表示 $\mathbb{P}$ 的唯一 约化格罗布讷基.

推论 5.3.4 设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中任一多项式组, 则

$$\mathrm{Zero}(\mathbb{P}) = \emptyset \iff \mathrm{GB}(\mathbb{P}) = [1].$$

证 若 $\mathrm{Zero}(\mathbb{P}) = \emptyset$, 则按照定理 1.6.2 有 $1 \in \mathrm{Ideal}(\mathbb{P})$. 因此 $\mathrm{Ideal}(\mathbb{P}) = \mathrm{Ideal}(\{1\})$. 于是依定理 5.3.3 有

$$\mathrm{GB}(\mathbb{P}) = \mathrm{GB}(\{1\}) = [1].$$

另一方面, $\mathrm{GB}(\mathbb{P}) = [1]$ 蕴涵着 $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}([1]) = \emptyset$. □

容易证明格罗布讷基的下述消元性质, 该性质由特英克斯首先观察获得. 它对依次确定零点尤为重要, 并将在下一章中扮演关键角色.

定理 5.3.5 设 $\mathbb{G}$ 为 $\mathcal{K}$ 上 —— 关于 $x_1 \prec \cdots \prec x_n$ 确定的纯字典项序 —— 的格罗布讷基, 那么对任意 $1 \le i \le n$ 有

$$\mathrm{Ideal}(\mathbb{G}) \cap \mathcal{K}[\boldsymbol{x}_i] = \mathrm{Ideal}(\mathbb{G} \cap \mathcal{K}[\boldsymbol{x}_i]), \tag{5.3.3}$$

式中右边的理想是在 $\mathcal{K}[\boldsymbol{x}_i]$ 中生成的.

证 (5.3.3) 式的左边明显包含其右边. 欲证其反向, 设 $G \in \mathrm{Ideal}(\mathbb{G}) \cap \mathcal{K}[\boldsymbol{x}_i]$, 则 $\mathrm{rem}(G, \mathbb{G}) = 0$. 注意, 在将 G 约化为 0 的过程中, 所有多项式都只牵涉到变元 $\boldsymbol{x}_i$. 因而, 对相应的余式公式 (5.3.1), 我们有

$$R = 0, \quad P_j \in \mathbb{G} \cap \mathcal{K}[\boldsymbol{x}_i], \quad Q_j \in \mathcal{K}[\boldsymbol{x}_i].$$

所以 G 属于 (5.3.3) 式的右边. □

格罗布讷序列

设 $G \in \mathbb{G}$ 为 $\mathcal{K}$ 上的可约多项式, 且有因子分解 $G = G_1 G_2$. 置 $\mathbb{P}_i = \mathbb{G} \cup \{G_i\}$; 又设 $\mathbb{G}_i$ 为 $\mathbb{P}_i$ 的格罗布讷基, $i = 1, 2$, 那么零点分解

$$\mathrm{Zero}(\mathbb{G}) = \mathrm{Zero}(\mathbb{G}_1) \cup \mathrm{Zero}(\mathbb{G}_2)$$

显然成立. 视每个 $\mathbb{G}_i$ 为 $\mathbb{G}$ 并如此继续, 我们将得到如下形式的分解:

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{G}_i), \tag{5.3.4}$$

这里 $\mathbb{G}_i$ 均为格罗布讷基, 且 $\mathbb{G}_i$ 中的所有多项式在 $\mathcal{K}$ 上都不可约.

定义 5.3.4 格罗布讷基 $\mathbb{G}_1, \cdots, \mathbb{G}_e$ 构成的有限集合或序列 Ψ 称为 $\mathcal{K}[\boldsymbol{x}]$ 中多项式组 $\mathbb{P}$ 的 *格罗布讷序列*, 如果零点分解 (5.3.4) 成立.

多项式系统 $[\mathbb{G}_1, \mathbb{D}_1], \cdots, [\mathbb{G}_e, \mathbb{D}_e]$ 构成的有限集合或序列 Ψ 称为 $\mathcal{K}[\boldsymbol{x}]$ 中多项式系统 $\mathfrak{P}$ 的 *格罗布讷序列*, 如果

$$\mathrm{Zero}(\mathfrak{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{G}_i / \mathbb{D}_i),$$

且每个 $\mathbb{G}_i$ 都是格罗布讷基. 当然可以假定 $0 \notin \mathrm{rem}(\mathbb{D}_i, \mathbb{G}_i)$ 对所有 i 成立.

Ψ 称为是 *拟不可约的*, 如果 $\mathbb{G}_i$ $(1 \le i \le e)$ 中的所有多项式在 $\mathcal{K}$ 上都不可约.

例 5.3.4 例 5.3.3 中格罗布讷基 $\mathbb{G}$ 的最后一个多项式在 $\mathbb{Q}$ 上是可约的. 按该多项式的因子分解将 $\mathbb{G}$ 分裂, 我们可得两个格罗布讷基

$$\begin{aligned}
\mathbb{G}_1 &= [2\,x_2^2 + 2\,x_1 x_2^2 - 2\,x_1 x_2 + x_1 + 1, x_3 - 2\,x_1 x_2 + x_1, x_4 + x_2 - 1], \\
\mathbb{G}_2 &= [2\,x_2^2 + 2\,x_1 x_2^2 - 2\,x_1 x_2 + x_1 + 1, x_3 + x_1 x_2 - x_1, x_4 - 2\,x_2 + 1],
\end{aligned}$$

使得

$$\mathrm{Zero}(\{P_1, G, P_3\}) = \mathrm{Zero}(\mathbb{G}_1) \cup \mathrm{Zero}(\mathbb{G}_2).$$

关于多项式 P_1, P_2, P_3 与 G, 见例 5.3.1 和 5.3.3. $\{P_1, P_2, P_3\}$ 的格罗布讷序列由下列两个格罗布讷基组成:

$$\begin{bmatrix} x_1^2x_2^2 + 4\,x_1x_2^2 + 2\,x_2^2 + x_1^3x_2 + 2\,x_1^2x_2 + x_1x_2 + x_1^2 + 2\,x_1 + 1, \\ x_1x_3 + x_3 - x_1x_2, \\ x_2x_3 + x_1x_2^2 + 2\,x_2^2 + x_1^2x_2 + x_1x_2 + x_1 + 1, \\ x_3^2 - 2\,x_2^2 - x_1x_2 - 1, \\ x_4 - x_3 \end{bmatrix},$$

$$\begin{bmatrix} 25\,x_1^3x_2^2 + 10\,x_1^2x_2^2 + 8\,x_2^2 + 4\,x_1x_2 + 4, \\ 2\,x_3 - 5\,x_1^2x_2 - 2\,x_1x_2, \\ 2\,x_4 + 5\,x_1x_2 \end{bmatrix}.$$

5.4 结 式 消 元

本节综述结式消元的主要 (经典) 技术. 我们的讨论将基于文献 [12, 39] 和 [71] (第十一章) 中的材料.

结式重观

我们已在 1.3 节中引进了西尔维斯特结式. 这里试将一元结式的另一构造描述如次. 该构造由贝佐和凯莱首先给出, 后来狄克逊[22] 将其推广到二元情形.

贝佐 - 凯莱结式

考虑两个一元多项式 $F, G \in \mathcal{R}[x]$, 其关于 x 的次数分别为 m 和 l, 这里和 1.3 节中一样, $m \geq l > 0$. 设 α 为一新的未定元. 行列式

$$\Delta(x, \alpha) = \begin{vmatrix} F(x) & G(x) \\ F(\alpha) & G(\alpha) \end{vmatrix}$$

是 x 和 α 的多项式, 且在 $x = \alpha$ 时为 0. 因此 $x - \alpha$ 是 Δ 的因子. 多项式

$$\Lambda(x, \alpha) = \frac{\Delta(x, \alpha)}{x - \alpha}$$

关于 α 的次数为 $m-1$, 并且关于 x 和 α 是对称的. 由于 $\Lambda(\bar{x},\alpha)=0$ 对任意 $\bar{x}\in \mathrm{Zero}(\{F,G\})$ 都成立, 无论 α 取值如何, 所以作为 α 的多项式 Λ 的所有系数 $B_i(x)=\mathrm{coef}(\Lambda,\alpha^i)$ 在 $x=\bar{x}$ 处都为 0. 考虑下列 m 个 x 的多项式方程:

$$B_0(x)=0,\cdots,B_{m-1}(x)=0, \tag{5.4.1}$$

B_i 关于 x 的最高次数为 $m-1$. F 和 G 的每个公共零点都是 (5.4.1) 的解, 而在 B_i 的系数矩阵之行列式 R 为 0 时, (5.4.1) 中的方程有公共解.

称 $m\times m$ 方阵的行列式 R 为 F 和 G 关于 x 的 贝佐－凯莱结式. 它与 1.3 节中定义的西尔维斯特结式在 $m=l$ 时恒同, 而在 $m>l$ 时相差一个多余因子 $\mathrm{lc}(F,x)^{m-l}$. 顺便指出, F 和 G 关于 x 的西尔维斯特结式是作为一个 $(l+m)\times(l+m)$ 方阵的行列式来构造的.

例 5.4.1 考虑一元四次多项式

$$F=x^4+x_1x^3+x_2x^2+x_3x+x_4.$$

我们希望计算 F 关于 x 的判别式, 它定义为 F 与其导数

$$G=\frac{dF}{dx}=4\,x^3+3\,x_1x^2+2\,x_2x+x_3$$

的结式. 按照上面的方法, 我们先计算

$$\Lambda=\frac{1}{x-\alpha}\begin{vmatrix} F(x) & G(x)\\ F(\alpha) & G(\alpha)\end{vmatrix}=G\alpha^3+B_2\alpha^2+B_1\alpha+B_0,$$

其中

$$\begin{aligned}
B_2&=3\,x_1x^3-(2\,x_2-3\,x_1^2)\,x^2-(3\,x_3-2\,x_1x_2)\,x-4\,x_4+x_1x_3,\\
B_1&=2\,x_2x^3-(3\,x_3-2\,x_1x_2)\,x^2-(4\,x_4+2\,x_1x_3-2\,x_2^2)\,x-3\,x_1x_4+x_2x_3,\\
B_0&=x_3x^3-(4\,x_4-x_1x_3)\,x^2-(3\,x_1x_4-x_2x_3)\,x-2\,x_2x_4+x_3^2.
\end{aligned}$$

命 Λ 中 α 的项的系数为 0, 我们得到四个方程

$$G=0,\quad B_2=0,\quad B_1=0,\quad B_0=0.$$

视为未定元 x^3, x^2, x^1, x^0 的齐次线性方程，它们有公共解当且仅当其系数矩阵行列式为 0, 即

$$\begin{aligned}R &= \begin{vmatrix} 4 & 3x_1 & 2x_2 & x_3 \\ 3x_1 & -2x_2+3x_1^2 & -3x_3+2x_1x_2 & -4x_4+x_1x_3 \\ 2x_2 & -3x_3+2x_1x_2 & -4x_4-2x_1x_3+2x_2^2 & -3x_1x_4+x_2x_3 \\ x_3 & -4x_4+x_1x_3 & -3x_1x_4+x_2x_3 & -2x_2x_4+x_3^2 \end{vmatrix} \\ &= 256x_4^3-192x_1x_3x_4^2-128x_2^2x_4^2+144x_1^2x_2x_4^2-27x_1^4x_4^2 \\ &\quad +144x_2x_3^2x_4-6x_1^2x_3^2x_4-80x_1x_2^2x_3x_4+18x_1^3x_2x_3x_4+16x_2^4x_4 \\ &\quad -4x_1^2x_2^3x_4-27x_3^4+18x_1x_2x_3^3-4x_1^3x_3^3-4x_2^3x_3^2+x_1^2x_2^2x_3^2 \\ &= 0.\end{aligned}$$

上面的行列式，即 F 的判别式，将在例 9.3.2 中用到.

狄克逊双次数结式

贝佐－凯莱结式的构造可以推广到三个关于变元 x 和 y 的双次数为 (l, m) 的多项式 F, G 和 H 以及其他限制情形. 这一点由狄克逊[22]所指出. 这里，**双次数**是指多项式 $F, G, H \in \mathcal{R}[x, y]$ 关于 x 和 y 的全次数为 $l+m$，但关于 x 的次数仅为 l，关于 y 的次数仅为 m. 让我们来考虑这一情形. 显而易见，行列式

$$\Delta(x, y, \alpha, \beta) = \begin{vmatrix} F(x,y) & G(x,y) & H(x,y) \\ F(\alpha,y) & G(\alpha,y) & H(\alpha,y) \\ F(\alpha,\beta) & G(\alpha,\beta) & H(\alpha,\beta) \end{vmatrix}$$

在用 x 替换 α 或 y 替换 β 之后为零. 因此 $(x-\alpha)(y-\beta) \mid \Delta$. 所以

$$\Lambda(x, y, \alpha, \beta) = \frac{\Delta(x, y, \alpha, \beta)}{(x-\alpha)(y-\beta)}$$

是 x, y, α, β 的多项式，而且

$$\begin{aligned}&\deg(\Lambda, \alpha) = 2l-1, \quad \deg(\Lambda, x) = l-1, \\ &\deg(\Lambda, \beta) = m-1, \quad \deg(\Lambda, y) = 2m-1.\end{aligned}$$

由于 $\Lambda(\bar{x}, \bar{y}, \alpha, \beta) = 0$ 对任意 $(\bar{x}, \bar{y}) \in \mathrm{Zero}(\{F, G, H\})$ 成立，无论 α 和 β 取值为何，因而系数 $D_{ij} = \mathrm{coef}(\Lambda, \alpha^i\beta^j)$ $(0 \le i \le 2l-1,\ 0 \le j \le m-1)$ 关于 x 和 y 有公共零点；这些零点构成的集合包含 $\mathrm{Zero}(\{F, G, H\})$. 将

$$D_{ij}(x, y) = 0 \quad (0 \le i \le l-1,\ 0 \le j \le 2m-1)$$

视为 $2lm$ 项

$$x^iy^j \quad (0 \le i \le l-1,\ 0 \le j \le 2m-1)$$

的 $2lm$ 个齐次线性方程. 写成矩阵形式, 我们有

$$\Lambda(x,y,\alpha,\beta) = (x^{l-1}y^{2m-1}\cdots y^{2m-1}\cdots x^{l-1}\cdots 1)\,\mathbf{D}\begin{pmatrix} \alpha^{2l-1}\beta^{m-1} \\ \vdots \\ \beta^{m-1} \\ \vdots \\ \alpha^{2l-1} \\ \vdots \\ 1 \end{pmatrix},$$

其中 $\mathbf{D}$ 是 D_{ij} 的系数矩阵. 矩阵 $\mathbf{D}$ 及其行列式 R 分别称为 $\{F,G,H\}$ 关于 x 和 y 的 *狄克逊矩阵* 和 *狄克逊结式*.

也可以对任意三个多项式 $F,G,H\in\mathcal{R}[x,y]$ 类似地构造相应的狄克逊矩阵 $\mathbf{D}$. 这时, $\mathbf{D}$ 不一定是方阵, 或者即使是方阵但可能是奇异的, 即 $\det(\mathbf{D})=0$. 因而该方法不总是适用. 然而, 只要狄克逊矩阵 $\mathbf{D}$ 是方阵且非奇异, $\mathbf{D}$ 的行列式与通常的结式就只相差一个常数因子; 称该行列式为 $\{F,G,H\}$ 关于 x 和 y 的 *狄克逊结式*. 我们用下面的例子来对此加以说明.

例 5.4.2 考虑二元三次多项式

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6.$$

多项式组

$$\mathbb{P} = \{F, \partial F/\partial x, \partial F/\partial y\}$$

关于 x 和 y 的结式 R 也称为 F 的 *判别式*; $R=0$ 给出三次曲线 $F(x,y)=0$ 有奇点的充分必要条件 (见 9.3 节). 若 $R\ne 0$, 则 $F(x,y)=0$ 为椭圆曲线.

为了求得 R, 我们首先计算多项式 $\Lambda(x,y,\alpha,\beta)$; 该多项式有 45 项, 并可写成如下形式

$$(xy\ \ y\ \ x^2\ \ x\ \ 1)$$

$$\cdot\begin{pmatrix} 0 & 6 & 0 & 3a_1 & 3a_3 \\ 6 & a_1^2+4a_2 & 6a_1 & d_{24} & d_{25} \\ 0 & 0 & -6 & d_{34} & d_{35} \\ 3a_1 & 3a_3 & 2a_1^2-4a_2 & d_{44} & d_{45} \\ 3a_3 & 2a_2a_3-a_1a_4 & 2a_1a_3-2a_4 & d_{54} & d_{55} \end{pmatrix}\cdot\begin{pmatrix} \alpha\beta \\ \beta \\ \alpha^2 \\ \alpha \\ 1 \end{pmatrix},$$

其中

$$
\begin{aligned}
d_{24} &= a_1^3 + 4\,a_1a_2 + 3\,a_3,\\
d_{25} &= a_1^2a_3 + 2\,a_2a_3 + a_1a_4,\\
d_{34} &= -a_1^2 - 4\,a_2,\\
d_{35} &= -a_1a_3 - 2\,a_4,\\
d_{44} &= -a_1^2a_2 - 4\,a_2^2 + 5\,a_1a_3 + 4\,a_4,\\
d_{45} &= -a_1a_2a_3 + 3\,a_3^2 - 2\,a_2a_4 + 6\,a_6,\\
d_{54} &= a_1a_2a_3 + 3\,a_3^2 - a_1^2a_4 - 2\,a_2a_4 + 6\,a_6,\\
d_{55} &= 2\,a_2a_3^2 - 2\,a_1a_3a_4 - 2\,a_4^2 + a_1^2a_6 + 4\,a_2a_6.
\end{aligned}
$$

上面的 5×5 矩阵的行列式

$$
\begin{aligned}
R = 18\,(&72\,a_2a_3^2a_4 + 288\,a_2a_4a_6 + 72\,a_1^2a_4a_6 - 8\,a_1^2a_2^2a_3^2 - 12\,a_1^4a_2a_6\\
&+ 8\,a_1^2a_2a_4^2 + 36\,a_1a_2a_3^3 - 30\,a_1^2a_3^2a_4 + 36\,a_1^3a_3a_6 - 96\,a_1a_3a_4^2\\
&- 48\,a_1^2a_2^2a_6 - a_1^4a_2a_3^2 + a_1^5a_3a_4 + a_1^4a_4^2 - a_1^6a_6 + a_1^3a_3^3\\
&+ 16\,a_1a_2^2a_3a_4 + 144\,a_1a_2a_3a_6 + 8\,a_1^3a_2a_3a_4 - 64\,a_4^3 - 27\,a_3^4\\
&+ 16\,a_2^2a_4^2 - 216\,a_3^2a_6 - 432\,a_6^2 - 64\,a_2^3a_6 - 16\,a_2^3a_3^2)
\end{aligned}
$$

含有 26 项；它是 $\mathbb{P}$ 关于 x 和 y 的狄克逊结式. 该结式可写为

$$R = 18\,(-b_2^2b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2b_4b_6),$$

其中

$$
\begin{aligned}
&b_2 = a_1^2 + 4\,a_2,\quad b_4 = a_1a_3 + 2\,a_4,\quad b_6 = a_3^2 + 4\,a_6,\\
&b_8 = a_1^2a_6 + 4\,a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.
\end{aligned}
$$

这是椭圆曲线理论中熟悉的表达式.

我们不再介绍三个等次数多项式和其他情形的狄克逊方法，也不再谈论其最新推广，如卡普尔、杨路等人的工作. 有关信息与技术性讨论，感兴趣的读者可参阅 [22, 12, 39, 40, 107] 及其所列文献.

多元结式

在这一小节里我们介绍麦考莱方法，它构造 n 个齐次多项式关于 n 个变元的结式；因而一次消去多个变元. 很清楚，这是一元和二元结式的推广. 同样，我们要构造关于 m 项的 m 个线性方程，而视这些项为不定元. 这种构造使用析配法：选取某些项并将其乘到所考虑的多项式上.

麦考莱矩阵

考虑一组关于 n 个变元 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 以不定元为系数的 n 个齐次多项式，设为 $\mathbb{P}=\{P_1,\cdots,P_n\}$，这里 $d_i=\operatorname{tdeg}(P_i)$. 令

$$d=1+\sum_{i=1}^{n}(d_i-1);$$

又置

$$\mathcal{M}=\{x_1^{i_1}\cdots x_n^{i_n}:\ i_1+\cdots+i_n=d\},$$

则

$$m=|\mathcal{M}|=\binom{d+n-1}{n-1}.$$

我们欲将每个多项式 P_i 乘上某些合适的项来生成 m 个项、次数为 d 的 m 个方程. 为此，命

$$\begin{aligned}\mathcal{M}_1&=\{\mu/x_1^{d_1}:\ x_1^{d_1}\mid\mu,\ \mu\in\mathcal{M}\},\\ \mathcal{M}_i&=\left\{\mu/x_i^{d_i}:\ x_i^{d_i}\mid\mu,\ \mu\in\mathcal{M}\setminus\{x_j^{d_j}\nu_j:\ \nu_j\in\mathcal{M}_j,1\le j\le i-1\}\right\},\\ &\qquad 2\le i\le n.\end{aligned}$$

又置 $m_i=|\mathcal{M}_i|$, $1\le i\le n$. 麦考莱在 [56] 中 (第 7 和 8 页) 证明了如下等式:

$$m_1+\cdots+m_n=m.$$

事实上，

$$\mathcal{M}=\{x_i^{d_i}\mu_i:\ \mu_i\in\mathcal{M}_i,1\le i\le n\}.$$

现在，我们构造一个 $m\times m$ 方阵 $\mathbf{M}$ 如次. 将 $\mathbf{M}$ 的列标上 $\mathcal{M}$ 中的项. 又将其前 m_1 行标上 $\mathcal{M}_1$ 中的项，接下来的 m_2 行标上 $\mathcal{M}_2$ 中的项，并照此进行. 在 $\mathcal{M}$ 的标有项 $\mu\in\mathcal{M}_i$ 的行、标有 ν 的列处 (对所有 $\nu\in\mathcal{M}$)，填入系数 $\operatorname{coef}(\mu P_i,\nu)$ (注意 $\operatorname{tdeg}(\mu P_i)=d$). 如此构造的矩阵 $\mathbf{M}$ 称为 $P_1,\cdots,P_n$，或 $\mathbb{P}$, 关于 $\boldsymbol{x}$ 的 *麦考莱矩阵*.

麦考莱结式

设 $\mathcal{N}_i$ 为 $\mathcal{M}_i$ 中那些能被至少某一 $x_j^{d_j}$ 整除的项构成的集合，这里 $2\le i+1\le j\le n$. 如果所有 $\mathcal{N}_i$ 皆为空集，那么命 $\mathbf{N}$ 为 1×1 阶平凡矩阵 (1). 否则，设 $\mathbf{N}$ 为 $\mathbf{M}$ 的子矩阵，其列标有

$$\{x_i^{d_i}\mu_i:\ \mu_i\in\mathcal{N}_i,1\le i\le n-1\}$$

中的项，而其行标有

$$\mathcal{N}_1 \cup \cdots \cup \mathcal{N}_{n-1}$$

中的项．M 的行列式关于每个 P_i 的系数都是齐次的．假定 N 的行列式非零 (见注 5.4.2)．定义商

$$R = \frac{\det(\mathbf{M})}{\det(\mathbf{N})}$$

为 $P_1, \cdots, P_n$ 或 $\mathbb{P}$ 关于 $\boldsymbol{x}$ 的 *麦考莱结式*.

现将以上讨论总结为如下算法.

算法 MacRes: $R \leftarrow \mathrm{MacRes}(\mathbb{P})$. 给定 $\mathcal{K}$ 上 (以未定元为系数) n 个变元 $\boldsymbol{x}$ 的 n 个齐次多项式组成的集合 $\mathbb{P} = \{P_1, \cdots, P_n\}$, 本算法计算 $\mathbb{P}$ 关于 $\boldsymbol{x}$ 的麦考莱结式 R.

M1. 命

$$d_i \leftarrow \mathrm{tdeg}(P_i), \quad i = 1, \cdots, n, \qquad d \leftarrow 1 + \textstyle\sum_{i=1}^{n}(d_i - 1),$$
$$\mathcal{M} \leftarrow \{x_1^{i_1} \cdots x_n^{i_n}:\ i_1 + \cdots + i_n = d\}, \quad \mathcal{T} \leftarrow \mathcal{M}, \quad \mathbb{M} \leftarrow \emptyset.$$

M2. 对 $i = 1, \cdots, n$ 执行下列步骤:

M2.1. 命

$$\mathcal{S} \leftarrow \{\mu \in \mathcal{T}:\ x_i^{d_i} \mid \mu\}, \quad \mathcal{M}_i \leftarrow \{\mu / x_i^{d_i}:\ \mu \in \mathcal{S}\}, \quad \mathcal{T} \leftarrow \mathcal{T} \setminus \mathcal{S}.$$

M2.2. 计算 $\mathbb{M} \leftarrow \mathbb{M} \cup \{\mu P_i:\ \mu \in \mathcal{M}_i\}$.

M3. 对 $i = 1, \cdots, n-1$ 命

$$\mathcal{N}_i \leftarrow \{\mu \in \mathcal{M}_i:\ \exists j,\ i+1 \le j \le n, \text{使 } x_j^{d_j} \mid \mu\}.$$

M4. 设 **M** 为 $\mathbb{M}$ 中的多项式以 $\mathcal{M}$ 中的项为变元的系数矩阵，且命

$$\mathcal{N} \leftarrow \mathcal{N}_1 \cup \cdots \cup \mathcal{N}_{n-1}.$$

若 $\mathcal{N} = \emptyset$, 则命 $\mathbf{N} \leftarrow (1)$; 否则，设 **N** 为 **M** 的子矩阵，其行标有 $\mathcal{N}$ 中的项而其列标有

$$\{x_i^{d_i}\mu_i:\ \mu_i \in \mathcal{N}_i, 1 \le i \le n-1\}$$

中的项．输出 $R \leftarrow \det(\mathbf{M}) / \det(\mathbf{N})$.

例 5.4.3 考虑下列三个以未定元为系数的三元多项式组成的集合 $\mathbb{P}$:

$$P_1 = a_{11}x_1^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{22}x_2^2 + a_{23}x_2x_3 + a_{33}x_3^2,$$
$$P_2 = b_{11}x_1^2 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{22}x_2^2 + b_{23}x_2x_3 + b_{33}x_3^2,$$
$$P_3 = c_1x_1 + c_2x_2 + c_3x_3.$$

使用上面的记号，我们有

$$d_1 = d_2 = 2,\quad d_3 = 1,\quad d = 3,\quad m = 10.$$

现将 10×10 麦考莱矩阵 $\mathbf{M}$ 以及所标记的项陈列如下：

$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_1 \\ x_2 \\ x_3 \\ x_1x_2 \\ x_1x_3 \\ x_2x_3 \\ x_3^2 \end{array}
\begin{array}{c}
\begin{array}{cccccccccc} x_1^3 & x_1^2x_2 & x_1^2x_3 & x_1x_2^2 & x_1x_2x_3 & x_1x_3^2 & x_2^3 & x_2^2x_3 & x_2x_3^2 & x_3^3 \end{array} \\
\begin{pmatrix}
a_{11} & a_{12} & a_{13} & a_{22} & a_{23} & a_{33} & 0 & 0 & 0 & 0 \\
0 & a_{11} & 0 & a_{12} & a_{13} & 0 & a_{22} & a_{23} & a_{33} & 0 \\
0 & 0 & a_{11} & 0 & a_{12} & a_{13} & 0 & a_{22} & a_{23} & a_{33} \\
b_{11} & b_{12} & b_{13} & b_{22} & b_{23} & b_{33} & 0 & 0 & 0 & 0 \\
0 & b_{11} & 0 & b_{12} & b_{13} & 0 & b_{22} & b_{23} & b_{33} & 0 \\
0 & 0 & b_{11} & 0 & b_{12} & b_{13} & 0 & b_{22} & b_{23} & b_{33} \\
0 & c_1 & 0 & c_2 & c_3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & c_1 & 0 & c_2 & c_3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_1 & 0 & 0 & c_2 & c_3 & 0 \\
0 & 0 & 0 & 0 & 0 & c_1 & 0 & 0 & c_2 & c_3
\end{pmatrix}
\end{array}.$$

它是按如下步骤构造的.

由于 $\mathbf{M}$ 头三列上标记的项能被 x_1^2 整除，故有 $\mathcal{M}_1 = \{x_1, x_2, x_3\}$. 将 P_1 分别乘上 $\mathcal{M}_1$ 中的 x_i 并填入相应的系数，我们得到 $\mathbf{M}$ 的头三行. 标在 $\mathbf{M}$ 的第四、第七和第八列上的项能被 x_2^2 整除，因而 $\mathcal{M}_2 = \{x_1, x_2, x_3\}$. 于是接下来的三行通过分别填入 x_1P_2, x_2P_2, x_3P_2 的系数而得. 用 x_3 除剩下四个标在列上的项给出

$$\mathcal{M}_3 = \{x_1x_2, x_1x_3, x_2x_3, x_3^2\}.$$

相应地，最后四行通过填入 μP_3 的系数 $(\mu \in \mathcal{M}_3)$ 获得.

$\mathbf{M}$ 的行列式是一个 432 项 a_{ij}, b_{ij} 和 c_k 的多项式. 至于 $\mathbf{M}$ 的相应子矩阵 $\mathbf{N}$, 我们不难求得 $\mathcal{N}_1 = \mathcal{N}_2 = \{x_3\}$. 选取 $\mathbf{M}$ 的第三和第八列以及第三和第六行给出 $\mathbf{N}$ 如下：

$$\begin{array}{c} \\ x_3 \\ x_3 \end{array}
\begin{array}{c}
\begin{array}{cc} x_1^2x_3 & x_2^2x_3 \end{array} \\
\begin{pmatrix} a_{11} & a_{22} \\ b_{11} & b_{22} \end{pmatrix}
\end{array}.$$

最终，我们得到 $\mathbb{P}$ 的麦考莱结式 $\det(\mathbf{M})/\det(\mathbf{N})$，一个 234 项 a_{ij}, b_{ij} 和 c_k 的多项式.

下述定理罗列了麦考莱结式的一些重要性质.

定理 5.4.1 设 $\mathbb{P}=\{P_1,\cdots,P_n\}$ 为一组 n 个 $\mathcal{K}$ 上以未定元为系数 $\boldsymbol{x}$ 的齐次多项式，R 为 $\mathbb{P}$ (关于 $\boldsymbol{x}$) 的麦考莱结式，而 $\mathbf{0}=(0,\cdots,0)$，那么

(a) $R=0$ 当且仅当 $\mathrm{Zero}(\mathbb{P}) \supsetneqq \{\mathbf{0}\}$;

(b) R 在 $\mathcal{K}$ 的任意代数闭包上不可约，并且在线性坐标变换下保持不变——因此 $R=0$ 是 $\mathrm{Zero}(\mathbb{P}) \supsetneqq \{\mathbf{0}\}$ 的最小必要条件;

(c) R 关于每个 P_i 的系数都是齐次的，其次数为 $\prod_{\substack{1\le j\le n\\ j\neq i}} d_j$，这里

$$d_i=\mathrm{tdeg}(P_i),\quad 1\le i\le n;$$

(d) 如果对某个 $1\le i\le n$ 及特定化的系数有 $P_i=FG$，则 R 为 $\mathbb{P}\setminus\{P_i\}\cup\{F\}$ 关于 $\boldsymbol{x}$ 的麦考莱结式 R_1 和 $\mathbb{P}\setminus\{P_i\}\cup\{G\}$ 关于 $\boldsymbol{x}$ 的麦考莱结式 R_2 的乘积.

证 见 [56] (第 8 至 15 页) 7 至 11 节. □

注 5.4.1 在所有 P_i 具有相同次数 (即 $d_1=\cdots=d_n$) 时，麦考莱在 [55] 中给出了一个构造 $\mathbb{P}$ 之结式的改进算法. 在这一情形，相应矩阵的阶数变得较小，见 [12]. 麦考莱的方法主要用来处理齐次多项式组及其在投影空间 $\mathbf{P}^n$ 中的零点. 对于非齐次多项式组，则需要在使用该方法之前将所考虑的多项式齐次化. 这时，无穷远处的零点也被包括在内; 对它们需要另加处理，如果我们只对仿射零点感兴趣.

注 5.4.2 麦考莱结式作为两个行列式的商只有在子矩阵 $\mathbf{N}$ 非奇异时才能定义. 非奇异条件在“一般”情形或者在多项式的系数为未定元时是能够满足的. 对于特定化的多项式，理论上的方法是先计算以未定元为系数的多项式的麦考莱结式 R，再将 R 中的未定元系数特定化 (即代入具体数值进行计算). 可是，这种方法实际上并不可行; 原因是即使多项式的次数较小，结式 R 也会很大. 对特定化的系数直接计算 R 又会遇到 $\mathbf{N}$ 奇异的情形. 为使方法实际可行，我们需要用摄动那样的先进技术 (见 [48] 和本节的结尾).

结式系统与 u结式

结式系统

同前，将 $x_1,\cdots,x_i$ 写成 $\boldsymbol{x}_i$，而 $\boldsymbol{x}=\boldsymbol{x}_n$. 又设

$$\mathbb{P}=\{P_1,\cdots,P_s\}$$

为 $\mathcal{K}[\boldsymbol{x}]$ 中 s (≥ 2) 个多项式构成的有限集合. 我们希望求得另一多项式组 $\mathbb{R}=\{R_1,\cdots,R_r\}\subset\mathcal{K}[\boldsymbol{x}_{n-1}]$ (其中变元 x_n 已消去)，并建立 $\mathbb{P}$ 与 $\mathbb{R}$ 之间的零点关系.

为此，令

$$d_i=\deg(P_i,x_n),\quad 1\leq i\leq s,\quad \text{且}\ d=\max_{1\leq i\leq s}d_i.$$

用 $x_n^{d-d_i}P_i$ 和 $(x_n-1)^{d-d_i}P_i$ 替换 $\mathbb{P}$ 中满足 $d_i<d$ 的那些 P_i，我们得到一个新的多项式组 $\mathbb{F}=\{F_1,\cdots,F_t\}$，使得 $\mathbb{F}$ 中的多项式关于 x_n 都有相同的次数 d，且 $\mathrm{Zero}(\mathbb{F})=\mathrm{Zero}(\mathbb{P})$. 对 x_n，我们构造两个多项式

$$F_1u_1+\cdots+F_tu_t,\quad F_1v_1+\cdots+F_tv_t$$

的结式 R，这里 $\boldsymbol{u}=(u_1,\cdots,u_t)$ 与 $\boldsymbol{v}=(v_1,\cdots,v_t)$ 都是新未定元. 显然，R 是 $\boldsymbol{x}_{n-1}$ 和 $\boldsymbol{u},\boldsymbol{v}$ 的多项式. 今视 R 为 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 的多项式，并设其非零系数为 $R_1,\cdots,R_e$. 称多项式组 $\mathbb{R}=\{R_1,\cdots,R_e\}\subset\mathcal{K}[\boldsymbol{x}_{n-1}]$ 为 $\mathbb{P}$ 关于 x_n 的*结式系统*. 在 $R\equiv 0$ 时，$\mathbb{R}$ 为空集. 依据范德瓦尔登 ([71] 第 1 页)，上述构造结式系统的方法应归功于克罗内克尔.

定理 5.4.2 设 $\mathbb{R}$ 为任一多项式组 $\mathbb{P}\subset\mathcal{K}[\boldsymbol{x}]$ 关于 x_n 的结式系统，而 $\bar{\boldsymbol{x}}_{n-1}\in\tilde{\mathcal{K}}^{n-1}$，那么 $\bar{\boldsymbol{x}}_{n-1}\in\mathrm{Zero}(\mathbb{R})$ 当且仅当或者

$$\mathrm{Zero}(\mathbb{P}^{\langle\bar{x},n-1\rangle})\neq\emptyset,\quad \text{或者}\ \ \bar{\boldsymbol{x}}_{n-1}\in\mathrm{Zero}(\{\mathrm{lc}(P,x_n):\ P\in\mathbb{P}\}).$$

证 设

$$F_u=F_1u_1+\cdots+F_tu_t,\quad F_v=F_1v_1+\cdots+F_tv_t$$

以及 $\mathbb{F}$ 如上. 由于 F_u 不依赖于 $\boldsymbol{v}$ 而 F_v 不依赖于 $\boldsymbol{u}$，所以 F_u 和 F_v 的每个公因子都一定不依赖于 $\boldsymbol{u}$ 和 $\boldsymbol{v}$，因此都整除 $F_1,\cdots,F_t$. 反之，$F_1,\cdots,F_t$ 的公因子也都整除 F_u 和 F_v. 故

$$\mathrm{Zero}(\mathbb{F})\neq\emptyset\iff\mathrm{Zero}(\{F_u,F_v\})\neq\emptyset.$$

设 $R = \mathrm{res}(F_u, F_v, x_n)$, 而 $\bar{\boldsymbol{x}}_{n-1} \in \tilde{\mathcal{K}}^{n-1}$. 由定理 1.3.2, $R(\boldsymbol{u}, \boldsymbol{v}, \bar{\boldsymbol{x}}_{n-1}) = 0$ 当且仅当 $F_u(\boldsymbol{u}, \bar{\boldsymbol{x}}_{n-1})$ 和 $F_v(\boldsymbol{v}, \bar{\boldsymbol{x}}_{n-1})$ 关于 x_n 有零点，或者

$$\mathrm{lc}(F_u, x_n)(\boldsymbol{u}, \bar{\boldsymbol{x}}_{n-1}) = \mathrm{lc}(F_v, x_n)(\boldsymbol{v}, \bar{\boldsymbol{x}}_{n-1}) = 0;$$

因而当且仅当

$$\mathrm{Zero}(\mathbb{P}^{\langle \bar{x}, n-1\rangle}) = \mathrm{Zero}(\{F_1, \cdots, F_t\}|_{\boldsymbol{x}_{n-1}=\bar{\boldsymbol{x}}_{n-1}}) \neq \emptyset,$$

或者

$$\bar{\boldsymbol{x}}_{n-1} \in \mathrm{Zero}(\{\mathrm{lc}(P, x_n)\colon\ P \in \mathbb{P}\}).$$

因 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 为未定元，故 $R(\boldsymbol{u}, \boldsymbol{v}, \bar{\boldsymbol{x}}_{n-1}) = 0$ 当且仅当作为 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 的多项式 R 的所有系数在 $\boldsymbol{x}_{n-1} = \bar{\boldsymbol{x}}_{n-1}$ 处都为零，即 $\bar{\boldsymbol{x}}_{n-1} \in \mathrm{Zero}(\mathbb{R})$. □

例 5.4.4　考虑多项式组 $\mathbb{P} = \{P_1, P_2, P_3\}$, 其中

$$P_1 = x - rt, \quad P_2 = y - rt^2, \quad P_3 = z - r^2.$$

这些多项式将在例 9.2.1 中再次出现. 今设变元序为 $x \prec y \prec z \prec t \prec r$. 欲求 $\mathbb{P}$ 关于 r 的结式系统，我们先构造下列多项式:

$$G_1 = rP_1, \quad G_2 = (r-1)\,P_1, \quad G_3 = rP_2, \quad G_4 = (r-1)\,P_2, \quad G_5 = P_3.$$

关于 r,

$$G_1u_1 + \cdots + G_5u_5 \quad 和 \quad G_1v_1 + \cdots + G_5v_5$$

的结式 R 为 x, y, z, t 和未定元 u_i, v_j 的多项式；该多项式含有 710 项. 收集 R 关于 u_i 和 v_j 的所有系数即得 $\mathbb{P}$ 的结式系统，它由 76 个 x, y, z 和 t 的多项式组成.

如范德瓦尔登在 [71] 中 (第 2 页) 所指出，如果 P_i 的形式导系数之一，比如说 $\mathrm{lc}(P_1, x_n)$, 不为零，那么 $\mathbb{F}$ 的构造是不需要的；此时可通过构造 P_1 和 $v_2P_2 + \cdots + v_nP_n$ 的结式较简单地获得结式系统.

对于例 5.4.4, $\mathrm{lc}(P_3, r) = -1 \neq 0$, 因而我们只需计算

$$\begin{aligned} R &= \mathrm{res}(P_3, v_1P_1 + v_2P_2, r) \\ &= -x^2v_1^2 - 2\,xyv_1v_2 - y^2v_2^2 + zt^2v_1^2 + 2\,zt^3v_1v_2 + zt^4v_2^2. \end{aligned}$$

收集 R (作为 v_1 和 v_2 的多项式) 的系数, 我们得到 $\mathbb{P}$ 的简单得多的结式系统如下:

$$\mathbb{R} = \{zt^2 - x^2, zt^4 - y^2, 2zt^3 - 2xy\}. \tag{5.4.2}$$

零点的确定

现在我们说明如何用结式系统确定任意多项式组 $\mathbb{P} = \{P_1, \cdots, P_s\}$ 的所有零点. 依照 [71] (第 3 页), 我们可以假定 $\mathbb{P}$ 含有一个多项式, 它关于 x_n 的导系数为非零常数. 如果该假定不成立, 则可按如下步骤使其成立. 撇开所有 P_i 都恒为零的平凡情形, 我们假定 —— 不失一般性 —— P_n 不恒为零. 在这一假设之下, 引进如下变元变换:

$$\begin{aligned} x_1 &= z_1 + u_1 z_n, \\ &\cdots\cdots \\ x_{n-1} &= z_{n-1} + u_{n-1} z_n, \\ x_n &= u_n z_n, \end{aligned}$$

这里 $\boldsymbol{u} = (u_1, \cdots, u_n)$ 为未定元或某些待定的特殊数值. 该变换将 P_n 变为另一多项式, 其关于 z_n 的导系数是 $\boldsymbol{u}$ 的非零多项式. $\boldsymbol{u}$ 可以取 $\mathcal{K}$ 或其某一扩域中的任意数值, 只要不使 P_n 的导系数为零.

令 $\mathbb{R}_n = \mathbb{P}$, 并假定 $\mathbb{R}_n$ 含有一多项式, 其关于 x_n 的导系数非零. 计算 $\mathbb{R}_n$ 的结式系统 $\mathbb{R}_{n-1} \subset \mathcal{K}[\boldsymbol{x}_{n-1}]$. 那么, 对任意 $\bar{\boldsymbol{x}}_{n-1} \in \mathrm{Zero}(\mathbb{R}_{n-1})$ 有 $\mathrm{Zero}(\mathbb{R}_n^{\langle \bar{x}, n-1 \rangle}) \neq \emptyset$. 事实上, 关于 x_n 的所有零点都可从 $\mathbb{R}_n^{\langle \bar{x}, n-1 \rangle}$ 中多项式的最大公因子求得.

因此, 我们的问题化为确定 $\mathbb{R}_{n-1}$ 的零点. 同样, 我们可以假定 $\mathbb{R}_{n-1}$ 含有一多项式, 其关于 x_{n-1} 的导系数非零, 并计算 $\mathbb{R}_{n-1}$ 的结式系统 $\mathbb{R}_{n-2} \subset \mathcal{K}[\boldsymbol{x}_{n-2}]$, 如此等等. 这样下去, 两种情形可能发生: 该过程或者在第 i 步停止, $i \leq n$, 使得 $\mathbb{R}_{n-i} = \{0\}$, 或者一直继续直到求得 $\mathbb{R}_0$, 而 $\mathbb{R}_0$ 中有一非零常数. 在后一情形, $\mathrm{Zero}(\mathbb{P}) = \emptyset$. 对于前者, 我们可以用任意数值替代结式系统 $\mathbb{R}_{n-i+1}, \cdots, \mathbb{R}_n$ 中的 $x_1, \cdots, x_{n-i}$, 再从代入后的结式系统依次求得关于 $x_{n-i+1}, \cdots, x_n$ 的零点. 零点的个数有限当且仅当 $i = n$. 如果在消元过程中作了线性变元变换, 则需要将新变元换回到原来的变元以获得原多项式组的零点.

鉴于结式系统的计算复杂性, 上述方法是不实用的. 依次消元本身颇为直接, 但使假设成立的变元变换将消元过程复杂化. 我们不再将该方法写成算法形式, 而仅用前面的例子来对其予以说明.

例 5.4.5　参见例 5.4.4. 对 (5.4.2) 中的 $\mathbb{R}$, 我们使用简单的变元变换 $z = w + t$, 那么 $\mathbb{R}$ 中的三个多项式变为

$$\begin{aligned} Q_1 &= (w+t)\,t^2 - x^2 = t^3 + wt^2 - x^2, \\ Q_2 &= (w+t)\,t^4 - y^2 = t^5 + wt^4 - y^2, \\ Q_3 &= 2\,(w+t)\,t^3 - 2\,xy = 2\,t^4 + 2\,wt^3 - 2\,xy, \end{aligned}$$

它们关于 t 的导系数都是常数. 多项式 Q_1 和 $v_2Q_2 + v_3Q_3$ 关于 t 的结式为 R_1R_2, 其中

$$\begin{aligned} R_1 &= x^5 - y^3 - xy^2w, \\ R_2 &= y^3v_2^3 + 6\,xy^2v_2^2v_3 - xy^2wv_2^3 - 4\,x^2ywv_2^2v_3 + 12\,x^2yv_2v_3^2 \\ &\quad - 4\,x^3wv_2v_3^2 + 8\,x^3v_3^3 + x^5v_2^3. \end{aligned}$$

由此可得 $\{Q_1, Q_2, Q_3\}$ 关于 t 的结式系统如下:

$$\mathbb{R}_1 = \left\{(x^5+y^3-xy^2w)\,R_1, 4\,x^2\,(3\,y-xw)\,R_1, 2\,xy\,(3\,y-2\,xw)\,R_1, 8\,x^3R_1\right\}.$$

由于 $\mathbb{R}_1$ 中的所有多项式有一公因子, $\mathbb{R}_1$ 关于 x, y, w 中任一变元的结式系统都应等于 $\{0\}$.

对 x 和 y 的任意给定值, 关于 w, t 和 r 的零点可依次从 $\mathbb{R}_1$, $\mathbb{R}$ 和 $\mathbb{P}$ 分别求得. 关于 z 的零点则以相应的 $w + t$ 而给出. 在一般情形, x 和 y 被视为未定元, 因而 $xy \neq 0$. $\mathbb{R}_1$ 中四个多项式的最大公因子为 R_1. 将 $R_1 = 0$ 对 w 求解得

$$w = \frac{x^5 - y^3}{xy^2}.$$

将这一解代入 Q_1, Q_2, Q_3 并计算其最大公因子, 我们得到关于 t 的仅有解: $t = y/x$. 现在可以给出关于 z 的解: $z = w + t = x^4/y^2$. 将关于 z 和 t 的解代入到 $\mathbb{P}$ 中原来的多项式并计算其最大公因子, 我们最后求得关于 r 的仅有解: $r = x^2/y$. 于是 $\mathbb{P}$ 关于 z, t, r 的仅有零点 (作为一般 x 和 y 的函数) 为

$$\left(\frac{x^4}{y^2}, \frac{y}{x}, \frac{x^2}{y}\right).$$

可解性判准

使用麦考莱结式, 我们已经建立了 n 个 n 元齐次多项式方程的可解性判别准则. 以下我们用结式系统导出任意多个齐次多项式方程可解性的代数判别准则.

在本节的余下部分, $\boldsymbol{x}$ 代表 $n+1$ 个变元 $x_0, x_1, \cdots, x_n$, 而 $\boldsymbol{x}_i = (x_0, x_1, \cdots, x_i)$; $\bar{\boldsymbol{x}}$, $\boldsymbol{u}$, $\boldsymbol{\lambda}$ 等为类似的缩写. 设 $P_1, \cdots, P_s$ 为 $\mathcal{K}$ 上以未定元为系数 $\boldsymbol{x}$ 的齐次非常数多项式. 它们总有"平凡"零点 $\mathbf{0} = (0, \cdots, 0)$. 因此判别准则是关于 $\mathbb{P} = \{P_1, \cdots, P_s\}$ 的非平凡零点的存在性. 下面的方法, 基于克罗内克尔的逐次消元法, 应归功于卡普费雷尔 (见 [71] 第 7 页).

按照上述方法 (但不作线性变元变换), 构造 $\mathbb{P}$ 关于 x_n 的结式系统 $\mathbb{R}$. 今欲证

$$\mathrm{Zero}(\mathbb{P}) \supsetneqq \{\mathbf{0}\} \iff \mathrm{Zero}(\mathbb{R}) \supsetneqq \{\mathbf{0}\} \tag{5.4.3}$$

在 $\mathcal{K}$ 的某一扩域中成立.

令 $d_i = \mathrm{tdeg}(P_i)$, $1 \le i \le s$. 首先考虑系数 $\mathrm{coef}(P_i, x_n^{d_i})$ 不全为零的情形. 依定理 5.4.2, 对 $\mathbb{R}$ 的每个非平凡零点 $\bar{\boldsymbol{x}}_{n-1}$, $\mathbb{P}^{\langle \bar{x}, n-1\rangle}$ 关于 x_n 至少有一个零点 $\bar{x}_n$. 零点 $\bar{\boldsymbol{x}}$ 当然不会是平凡的. 反之, $\mathbb{P}$ 的每个非平凡零点 $\bar{\boldsymbol{x}}$ 都给出 $\mathbb{R}$ 的一个零点 $\bar{\boldsymbol{x}}_{n-1}$; 由于 $\bar{\boldsymbol{x}}_{n-1} = 0$ 会立即导致 $\bar{x}_n = 0$ (注意: 每个 P_i 都是齐次的), 该零点也不能平凡.

如果 $\mathrm{coef}(P_i, x_n^{d_i})$ 对所有 i 都为零, 那么按照定理 5.4.2 有 $\mathbb{R} = \emptyset$. 所以 $\mathbb{R}$ 有一非平凡零点, 譬如说 $(1, \cdots, 1)$. 这时, $(0, \cdots, 0, 1)$ 是 $\mathbb{P}$ 的一个非平凡零点 (由于 P_i 不含有 x_n 的最高次幂项). 于是 (5.4.3) 获证.

现在 $\mathbb{R}$ 中的多项式, 如果有的话, 关于 $\boldsymbol{x}_{n-1}$ 都是齐次的, 因此我们可以构造 $\mathbb{R}$ 关于 x_{n-1} 的结式系统. 让这一消元过程对 $x_{n-1}, \cdots, x_1$ 继续. 我们最终将得到一组 x_0 的齐次多项式

$$R_1 x_0^{k_1}, \cdots, R_t x_0^{k_t}. \tag{5.4.4}$$

这些多项式有非平凡零点当且仅当 $R_1 = \cdots = R_t = 0$.

显然, $R_1, \cdots, R_t$ 是 P_i 的系数的多项式. 由其构造, 容易证明它们关于单个 P_i 的系数都是齐次的 (见 [71] 第 8 页). 多项式组 $\{R_1, \cdots, R_t\}$ 也称为 $P_1, \cdots, P_s$ 或 $\mathbb{P}$ 关于 $\boldsymbol{x}$ 的 结 式 系 统. 它有可能为空集: 是时 $t = 0$.

总结以上讨论, 我们有如下定理.

定理 5.4.3 从 $\mathcal{K}$ 上任意以未定元 $\boldsymbol{u}$ 为系数、$\boldsymbol{x}$ 的齐次多项式组 $\mathbb{P}$, 可以求得 $\mathcal{K}[\boldsymbol{u}]$ 中的多项式组 $\mathbb{R}$, 使得对 $\boldsymbol{u}$ 在 $\mathcal{K}$ 的任一扩域中的特殊值 $\bar{\boldsymbol{u}}$,

$$\bar{\boldsymbol{u}} \in \mathrm{Zero}(\mathbb{R}) \iff \mathrm{Zero}(\mathbb{P}|_{\boldsymbol{u}=\bar{\boldsymbol{u}}}) \supsetneqq \{\mathbf{0}\}.$$

$\mathbb{R}$ 中的多项式关于 $\mathbb{P}$ 中单个多项式的系数都是齐次的.

$\mathbb{P}$ 的结式系统 $\mathbb{R}$ 中可能含有大量多项式. 定理 5.4.1 表明, 在 $|\mathbb{P}| = s = n+1$ (变元的个数) 时, 单个麦考莱结式就足够了. 一般说来, 在 $s < n+1$ 时可解性是无条件的.

u 结式

考虑一组 n 个齐次多项式

$$\mathbb{P} = \{P_1, \cdots, P_n\} \subset \mathcal{K}[\boldsymbol{x}].$$

令 $d_i = \mathrm{tdeg}(P_i)$, $1 \le i \le n$, 并置

$$P_u = x_0u_0 + x_1u_1 + \cdots + x_nu_n,$$

这里 $\boldsymbol{u} = (u_0, u_1, \cdots, u_n)$ 为 $n+1$ 个新未定元.

定义 5.4.1　称 $n+1$ 个齐次多项式

$$P_1, \cdots, P_n, P_u$$

关于 $n+1$ 个变元 $\boldsymbol{x}$ 的麦考莱结式 R_u 为 $P_1, \cdots, P_n$ 或 $\mathbb{P}$ 关于 $\boldsymbol{x}$ 的 u 结式.

也可以对任意 s (不一定是 n) 个 $\boldsymbol{x}$ 的、仅有有限多个零点的齐次多项式定义 u 结式 (见 [71] 第 15 和 16 页). 对 $n = 2$, u 结式亦可通过二元结式来构造 (参见 [12]).

设 R_u 为 $\mathbb{P}$ —— $\mathcal{K}[\boldsymbol{x}]$ 中一组 n 个齐次多项式 —— 关于 $\boldsymbol{x}$ 的 u 结式. 若 $R_u \equiv 0$, 则 $\mathrm{Zero}(\mathbb{P})$ 为无限集. 否则, 依定理 5.4.1 (c) R_u 是 $\boldsymbol{u}$ 的齐次多项式, 其次数为 $D = d_1 \cdots d_n$. 这时, 可将 R_u 在 $\mathcal{K}$ 的某一代数扩域上分解为线性因子:

$$R_u = \prod_{j=1}^{D} (\lambda_{0j}u_0 + \lambda_{1j}u_1 + \cdots + \lambda_{nj}u_n).$$

因此, 对任意 $1 \le j \le D$ 有

$$(\lambda_{0j}, \lambda_{1j}, \cdots, \lambda_{nj}) \in \mathrm{Zero}(\mathbb{P}). \tag{5.4.5}$$

反之, 若 (5.4.5) 成立, 则

$$\lambda_{0j}u_0 + \lambda_{1j}u_1 + \cdots + \lambda_{nj}u_n$$

必为 R_u 的因子. 这就给出了一个方法, 它可以确定 Zero($\mathbb{P}$) 以及每个零点的重数 (作为相应线性因子的次数) (参阅 [48]).

为说明上述方法的正确性, 考虑任意

$$\bar{\boldsymbol{x}} = (\bar{x}_0, \bar{x}_1, \cdots, \bar{x}_n) \in \mathrm{Zero}(\mathbb{P}).$$

对任意满足

$$\bar{x}_0\bar{u}_0 + \bar{x}_1\bar{u}_1 + \cdots + \bar{x}_n\bar{u}_n = 0 \tag{5.4.6}$$

的 $\bar{\boldsymbol{u}} = (\bar{u}_0, \bar{u}_1, , \cdots, \bar{u}_n)$, 线性方程 $P_{\bar{u}} = 0$ 表示经过点 $\bar{\boldsymbol{x}}$ 的超平面. 由此可见

$$\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{P} \cup \{P_{\bar{u}}\}).$$

所以, 依定理 5.4.1 (a) 有 $R_{\bar{u}} = 0$. 由于这对任意满足 (5.4.6) 的 $\bar{\boldsymbol{u}}$ 都成立, 故由多项式的整除性可知

$$\bar{x}_0 u_0 + \bar{x}_1 u_1 + \cdots + \bar{x}_n u_n$$

是 R_u 的因子.

对 R_u 的任意线性因子

$$L = \lambda_0 u_0 + \lambda_1 u_1 + \cdots + \lambda_n u_n,$$

我们称所有 R_u 的那些与 L 只差 ($\mathcal{K}$ 的某一代数扩域中的) 常数因子的线性因子 (包括 L 本身) 的个数为

$$(\lambda_0, \lambda_1, \cdots, \lambda_n) \in \mathrm{Zero}(\mathbb{P})$$

的 **重数**. 作为推论, 我们有下述构造性的贝佐定理.

定理 5.4.4 设 $\mathbb{P}$ 为一组 n 个 $\mathcal{K}[\boldsymbol{x}]$ 中的齐次多项式, 那么或者 Zero($\mathbb{P}$) 为无限集, 或者所有 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{P})$ 的重数的总和等于 $\prod_{P\in\mathbb{P}} \mathrm{tdeg}(P)$.

如果所给多项式 P_i 是非齐次的, 即通常关于 n 个变元 $x_1, \cdots, x_n$ 的多项式, 我们可以引进一个新变元 x_0 将它们齐次化. 设所得的齐次多项式组为

$$\tilde{\mathbb{P}} = \{\tilde{P}_1, \cdots, \tilde{P}_n\}.$$

因为不太会引起混淆, $\tilde{\mathbb{P}}$ 的 u 结式 R_u 亦称为 $\mathbb{P}$ 的 **u 结式**. 我们也可以用 R_u 来确定 Zero($\mathbb{P}$). 下例对此予以说明.

例 5.4.6　求由下列方程分别给出的圆和椭圆的交点:

$$P_1 = x_1^2 + x_2^2 - 2 = 0,$$
$$P_2 = x_1^2 + 6\,x_2^2 - 3 = 0.$$

为此，我们计算 $\{P_1, P_2\}$ 关于 x_1 和 x_2 的 u 结式 R. 根据定义，R 是

$$\tilde{P}_1 = x_1^2 + x_2^2 - 2\,x_0^2,$$
$$\tilde{P}_2 = x_1^2 + 6\,x_2^2 - 3\,x_0,$$
$$P_u = u_0 x_0 + u_1 x_1 + u_2 x_2$$

的麦考莱结式；上式中引入了 x_0 以将 P_1 和 P_2 齐次化. 在例 5.4.3 所计算的麦考莱结式中，命 $x_3 = x_0$, 并用 $\tilde{P}_1, \tilde{P}_2$ 的数值系数替换相应的 a_{ij}, b_{ij}, 用 u_i 替换 c_i (当然 $u_3 = u_0$), 由此可得

$$R = 25\,u_0^4 - 90\,u_0^2 u_1^2 - 10\,u_0^2 u_2^2 + 81\,u_1^4 - 18\,u_1^2 u_2^2 + u_2^4.$$

该多项式可分解为

$$\left(\sqrt{5}\,u_0 + 3\,u_1 + u_2\right)\left(\sqrt{5}\,u_0 + 3\,u_1 - u_2\right)\cdot$$
$$\left(\sqrt{5}\,u_0 - 3\,u_1 + u_2\right)\left(\sqrt{5}\,u_0 - 3\,u_1 - u_2\right).$$

从这些线性因子，我们立即得到四个交点

$$\left(\frac{3}{\sqrt{5}}, \frac{1}{\sqrt{5}}\right),\quad \left(\frac{3}{\sqrt{5}}, -\frac{1}{\sqrt{5}}\right),\quad \left(-\frac{3}{\sqrt{5}}, \frac{1}{\sqrt{5}}\right),\quad \left(-\frac{3}{\sqrt{5}}, -\frac{1}{\sqrt{5}}\right).$$

上述基于计算 $\mathbb{P}$ 的 u 结式 R_u 来确定 Zero($\mathbb{P}$) 的方法只在 $R_u \neq 0$ (即 Zero($\tilde{\mathbb{P}}$) 有限) 时才适用. 可能发生的是 Zero($\mathbb{P}$) 有限，而 Zero($\tilde{\mathbb{P}}$) 无限. 换言之，$\mathbb{P}$ 可能有无限多个零点在无穷远处. 因此 R_u 甚至在 Zero($\mathbb{P}$) 有限时也会恒等于 0. 如果这种情形发生了，我们说 Zero($\mathbb{P}$) 有 *超分支* 在无穷远处. 举例来说，令

$$\mathbb{P} = \{x_1(x_1 + \cdots + x_n) - 1, \cdots, x_n(x_1 + \cdots + x_n) - 1\};$$

Zero($\mathbb{P}$) 含有两个 (仿射) 零点

$$\left(\frac{1}{\sqrt{n}}, \cdots, \frac{1}{\sqrt{n}}\right),\quad \left(-\frac{1}{\sqrt{n}}, \cdots, -\frac{1}{\sqrt{n}}\right),$$

并在 $n \geq 2$ 时有一个由 $x_1+\cdots+x_n=0$ 给出的超分支在无穷远处. 对 $n \geq 3$, $\mathbb{P}$ 的 u 结式 R_u 为零. 在 $n=2$ 时, 因齐次化的多项式组 $\tilde{\mathbb{P}}$ 只有有限多个零点, 故 R_u 非零.

为了处理那些仅有有限多个仿射零点但有超分支在无穷远处的非齐次多项式组, 我们可以使用上述方法的修正版, 它能求得所有仿射零点. 按照文献[39], 下面介绍的修正应归功于坎尼, 奇斯托夫和格里高里夫.

考虑任意一组 n 个多项式: $\mathbb{P}=\{P_1,\cdots,P_n\}\subset \mathcal{K}[x_1,\cdots,x_n]$. 设 $\tilde{P}_i$ 是用 x_0 齐次化 P_i 所得的多项式, 且命

$$F_i=\tilde{P}_i+vx_i^{d_i},\quad 1\leq i\leq n,$$
$$F_u=(u_0+v)\,x_0+u_1x_1+\cdots+u_nx_n,$$

其中 v 为一新变元. 视 $F_1,\cdots,F_n,F_u$ 为 $x_0,x_1,\cdots,x_n$ 的齐次多项式, 并计算其麦考莱结式 $R_u=R_u(v,\boldsymbol{u})$; 称 R_u 为 $\mathbb{P}$ 关于 $x_1,\cdots,x_n$ 的 *广义特征多项式*. 今视 R_u 为 v 的多项式, 并将其写成如下形式:

$$R_u=v^q+R_{q-1}v^{q-1}+\cdots+R_kv^k,$$

这里 $k\geq 0$, 而 R_i 为 $\mathcal{K}[\boldsymbol{u}]$ 中的多项式. 若 $k=0$, 则 R_k 与 $\mathbb{P}$ 的 u 结式 R_u 相同. 若 $\mathbb{P}$ 有超分支在无穷远处, 则 $k>0$. 在这后一种情形, 尾系数 R_k 与 R_u 有同样良好的性质: R_k 可在 $\mathcal{K}$ 的某一代数扩域上分解为线性因子,

$$R_k=\prod_j(\lambda_{0j}u_0+\lambda_{1j}u_1+\cdots+\lambda_{nj}u_n),$$

因此对每个 j 有

$$(\lambda_{0j},\lambda_{1j},\cdots,\lambda_{nj})\in \mathrm{Zero}(\tilde{\mathbb{P}}).$$

反之, 若 $(\bar{x}_1,\cdots,\bar{x}_n)\in \mathrm{Zero}(\mathbb{P})$, 则

$$u_0+\bar{x}_1u_1+\cdots+\bar{x}_nu_n$$

为 R_k 的因子. 这就提供了一条获得 $\mathbb{P}$ 的所有仿射零点的途径, 尽管超分支有可能出现在无穷远处.

注 5.4.3 对中等大小的多项式组计算完全的 u 结式因而完全的广义特征多项式几乎是不可能的. 关于零点的实际计算, 我们可以用特定的值来代替某些未定元 u_i 然后再构造 u 结式, 以便先对某些变元确定零点. 这类技巧来自最新研究. 关于具体细节, 有兴趣的读者可参阅坎尼、拉克施曼及其合作者的有关著作.

第六章 计算代数几何与多项式理想论

代数几何研究的基本对象之一是代数簇，它是多项式组的零点 —— 视为仿射空间中点 —— 的集合. 与之相应，多项式组生成的理想是交换代数中所处理的典型实体. 消去法为这两个相关领域中的诸多问题提供了强有力的构造性工具. 本章研究几个此类问题，重点在其计算方面.

6.1 维 数

如同前几章中那样，所考虑的多项式都是关于 n 个变元 $\boldsymbol{x}$, 其系数属于一个固定的、特征为 0 的数域 $\mathcal{K}$, 除非另有说明.

定义 6.1.1 完美三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 的 **维数** 定义为

$$\dim(\mathbb{T}) \triangleq n - |\mathbb{T}|.$$

它也称为 $\mathcal{K}[\boldsymbol{x}]$ 中任意完美三角系统 $[\mathbb{T}, \mathbb{U}]$ 的 **维数**.

引理 6.1.1 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意完美三角系统 $\mathfrak{T}$, 可以求得 $\mathfrak{T}$ 的不可约三角序列 Ψ, 使得

$$\dim(\mathfrak{T}) = \max_{\mathfrak{T}^* \in \Psi} \dim(\mathfrak{T}^*).$$

证 将算法 Decom 用于 $\mathfrak{T} = [\mathbb{T}, \mathbb{U}]$, 我们可得 $[\mathbb{T}_1, \mathbb{U}_1], \cdots, [\mathbb{T}_e, \mathbb{U}_e]$ 和 $[\mathbb{P}_1, \mathbb{Q}_1, \mathbb{T}_1^*], \cdots, [\mathbb{P}_h, \mathbb{Q}_h, \mathbb{T}_h^*]$ 使 (4.4.4) 成立，且每个不可约三角列 $\mathbb{T}_i$ 与 $\mathbb{T}$ 都具有相同的参量；因此 $\dim(\mathbb{T}_i) = \dim(\mathbb{T})$. 假定在 Decom 的 D2.2.2 中，对所有 T 的代数因子分解，多项式 D 的选取都不是随意的而是使其不含有 $\mathbb{T}'$ 的依量. 于是 (4.4.4) 中的每个 $\mathbb{P}_j$ 实际上都是从三角列 $\mathbb{T}_j^-$ 通过添加单个多项式 D_j 而得到的. 此外，$\mathbb{T}_j^-$ 与 $\mathbb{T}$ 具有相同的参量，而且 D_j 只含有这些参量. 设

$$[\mathbb{T}_{j1}, \mathbb{U}_{j1}], \cdots, [\mathbb{T}_{jt_j}, \mathbb{U}_{jt_j}]$$

为 $\{D_j\}$ 的三角序列，而 $\mathbb{T}_{jl}^* = \mathbb{T}_{jl} \cup \mathbb{T}_j^- \cup \mathbb{T}_j^*$, $l = 1, \cdots, t_j$, 那么

$$\operatorname{Zero}(\mathbb{P}_j \cup \mathbb{T}_j^* / \mathbb{Q}_j) = \bigcup_{l=1}^{t_j} \operatorname{Zero}(\mathbb{T}_{jl}^* / \mathbb{Q}_j \cup \mathbb{U}_{jl}),$$

每个 $\mathbb{T}_{jl}^*$ 都可排为三角列，并且 $\mathfrak{T}_{jl} = [\mathbb{T}_{jl}^*, \mathbb{Q}_j \cup \mathbb{U}_{jl}]$ 为三角系统．若 $\mathfrak{T}_{jl}$ 完美，则 $\dim(\mathfrak{T}_{jl}) < \dim(\mathbb{T})$．现将每个完美三角系统 $\mathfrak{T}_{jl}$ 视作 $[\mathbb{T}, \mathbb{U}]$，并按以上方式递归进行．这一程序最后将会终止，以给出 $\mathfrak{T}$ 的不可约三角序列 Ψ．这就证明了

$$\dim(\mathfrak{T}) \geq \max_{\mathfrak{T}^* \in \Psi} \dim(\mathfrak{T}^*).$$

余下的是要说明 $e \neq 0$．依引理 3.2.3, $\mathfrak{T}$ 有正则零点 $\boldsymbol{\xi}$．若 $e = 0$，则对任意 $[\mathbb{T}^*, \mathbb{U}^*] \in \Psi$, $\mathbb{T}^*$ 的参量的个数都比 $\mathbb{T}$ 的参量的个数小．所以，$\boldsymbol{\xi}$ 不可能是一个这样的三角系统 $[\mathbb{T}^*, \mathbb{U}^*]$ 的零点．由此导出矛盾，故 $e > 0$．引理获证． □

推论 6.1.2 对 $\mathcal{K}[\boldsymbol{x}]$ 中任意完美三角系统 $\mathfrak{T}$ 的不可约三角序列 Ψ,

$$\dim(\mathfrak{T}) = \max_{\mathfrak{T}^* \in \Psi} \dim(\mathfrak{T}^*).$$

证 按引理 6.1.1 计算 $\mathfrak{T}$ 的不可约三角序列 $\bar{\Psi}$, 使得

$$\dim(\mathfrak{T}) = \max_{\bar{\mathfrak{T}} \in \bar{\Psi}} \dim(\bar{\mathfrak{T}}).$$

显而易见,

$$\bigcup_{\bar{\mathfrak{T}} \in \bar{\Psi}} \mathrm{Zero}(\bar{\mathfrak{T}}) = \bigcup_{\mathfrak{T}^* \in \Psi} \mathrm{Zero}(\mathfrak{T}^*) \tag{6.1.1}$$

成立．若

$$\max_{\bar{\mathfrak{T}} \in \bar{\Psi}} \dim(\bar{\mathfrak{T}}) > \max_{\mathfrak{T}^* \in \Psi} \dim(\mathfrak{T}^*),$$

则存在 $\bar{\mathfrak{T}} \in \bar{\Psi}$, 使得 $\dim(\bar{\mathfrak{T}}) > \dim(\mathfrak{T}^*)$ 对所有 $\mathfrak{T}^* \in \Psi$ 成立．设 $\boldsymbol{\xi} \in \mathrm{RegZero}(\bar{\mathfrak{T}})$, 那么 $\boldsymbol{\xi}$ 不能是任一 $\mathfrak{T}^* \in \Psi$ 的零点．这与 (6.1.1) 相矛盾．基于同样理由， $\max_{\bar{\mathfrak{T}} \in \bar{\Psi}} \dim(\bar{\mathfrak{T}})$ 不能比 $\max_{\mathfrak{T}^* \in \Psi} \dim(\mathfrak{T}^*)$ 小．所以,

$$\dim(\mathfrak{T}) = \max_{\bar{\mathfrak{T}} \in \bar{\Psi}} \dim(\bar{\mathfrak{T}}) = \max_{\mathfrak{T}^* \in \Psi} \dim(\mathfrak{T}^*).$$

证毕． □

引理 6.1.3 $\mathcal{K}[\boldsymbol{x}]$ 中的任意完美三角系统在 $\mathcal{K}$ 的代数闭包上也是完美的．

证　设 $\mathfrak{T}$ 为完美三角系统，而 Ψ 为 $\mathfrak{T}$ 的不可约三角序列，则 $\Psi \neq \emptyset$. 设 $\mathfrak{T}^* \in \Psi$. 依定理 4.5.3, $\mathfrak{T}^*$ 在 $\mathcal{K}$ 的代数闭包 $\bar{\mathcal{K}}$ 中有零点．该零点也是 $\mathfrak{T}$ 的零点．所以 $\mathfrak{T}$ 在 $\bar{\mathcal{K}}$ 上是完美的. □

推论 6.1.4　$\mathcal{K}[\boldsymbol{x}]$ 中的任意三角系统是完美的当且仅当它在 $\mathcal{K}$ 的代数闭包上是完美的.

定理 3.2.13 也可视为引理 6.1.3 的推论.

记号：ITS($\mathfrak{P}$) 表示 $\mathcal{K}[\boldsymbol{x}]$ 中任一多项式组或系统 $\mathfrak{P}$ 的 不可约三角序列.

引理 6.1.5　设 Ψ_1 和 Ψ_2 为 $\mathcal{K}[\boldsymbol{x}]$ 中的三角序列，其中所有三角系统都是完美的，使得

$$\bigcup_{\mathfrak{T}_1 \in \Psi_1} \mathrm{Zero}(\mathfrak{T}_1) = \bigcup_{\mathfrak{T}_2 \in \Psi_2} \mathrm{Zero}(\mathfrak{T}_2),$$

那么

$$\max_{\mathfrak{T}_1 \in \Psi_1} \dim(\mathfrak{T}_1) = \max_{\mathfrak{T}_2 \in \Psi_2} \dim(\mathfrak{T}_2).$$

证　注意：

$$\Psi_i^* = \bigcup_{\mathfrak{T}_i \in \Psi_i} \mathrm{ITS}(\mathfrak{T}_i) \quad (i = 1, 2)$$

为两个不可约三角序列，使得

$$\bigcup_{\mathfrak{T}_1 \in \Psi_1^*} \mathrm{Zero}(\mathfrak{T}_1) = \bigcup_{\mathfrak{T}_2 \in \Psi_2^*} \mathrm{Zero}(\mathfrak{T}_2).$$

由推论 6.1.2, 对 $i = 1, 2$ 有

$$\max_{\mathfrak{T}_i \in \Psi_i} \dim(\mathfrak{T}_i) = \max_{\mathfrak{T}_i \in \Psi_i} \max_{\mathfrak{T}_i^* \in \mathrm{ITS}(\mathfrak{T}_i)} \dim(\mathfrak{T}_i^*) = \max_{\mathfrak{T} \in \Psi_i^*} \dim(\mathfrak{T}).$$

重复推论 6.1.2 证明中的推理可见

$$\max_{\mathfrak{T}_1 \in \Psi_1^*} \dim(\mathfrak{T}_1) = \max_{\mathfrak{T}_2 \in \Psi_2^*} \dim(\mathfrak{T}_2).$$

由此即得

$$\max_{\mathfrak{T}_1 \in \Psi_1} \dim(\mathfrak{T}_1) = \max_{\mathfrak{T}_2 \in \Psi_2} \dim(\mathfrak{T}_2).$$

□

作为该引理的推论，我们有如下结果.

推论 6.1.6 设 Ψ 为 $\mathcal{K}[\boldsymbol{x}]$ 中完美三角系统 $\mathfrak{T}$ 的任意三角序列，其中所有三角系统都是完美的，那么

$$\dim(\mathfrak{T}) = \max_{\mathfrak{T}^* \in \Psi} \dim(\mathfrak{T}^*).$$

由引理 6.1.5, 以下定义是适当的.

定义 6.1.2 设 $\mathfrak{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统，$\text{Zero}(\mathfrak{P}) \neq \emptyset$, 而 Ψ 为 $\mathfrak{P}$ 的任意三角序列，其中所有三角系统都是完美的. $\mathfrak{P}$ 的 *维数* 定义为

$$\text{Dim}(\mathfrak{P}) \triangleq \max_{\mathfrak{T} \in \Psi} \dim(\mathfrak{T}).$$

也称 $\text{Dim}([\mathbb{P}, \emptyset])$ 为 $\mathbb{P}$ 的 *维数*.

注 6.1.1 我们将记号 Dim 中的 D 大写以区别多项式组 (系统) 的维数与三角列 (系统) 的维数. 例如，在 4 维空间中考虑

$$\mathbb{T} = [x\,(x-1), xy+u, xz-u],$$

这里 $u \prec x \prec y \prec z$. 作为多项式组，$\mathbb{T}$ 的维数明显为 2. 可是，作为三角列 $\mathbb{T}$ 是完美的，且维数为 $4 - |\mathbb{T}| = 1$. 所以

$$\text{Dim}(\mathbb{T}) = 2 \neq 1 = \dim(\mathbb{T}).$$

代数簇 或 *流形* 是 n 维空间中由代数方程组定义的几何对象. 现在我们引进几个有关代数簇的概念.

定义 6.1.3 设 $\mathbf{A}^n_{\tilde{\mathcal{K}}}$ 为 $\mathcal{K}$ 的某一扩域 $\tilde{\mathcal{K}}$ 上以 $\boldsymbol{x}$ 为坐标的 n 维仿射空间，而 $\mathcal{V}$ 为 $\mathbf{A}^n_{\tilde{\mathcal{K}}}$ 中点的集合. 如果存在多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 使得 $\mathcal{V} = \text{Zero}(\mathbb{P})$, 则称 $\mathcal{V}$ 为 (仿射) *代数簇*. 我们又称 $\mathbb{P}$ 为 $\mathcal{V}$ 的 *定义多项式组*, $\mathbb{P} = 0$ 为 $\mathcal{V}$ 的 *定义方程组*.

称代数簇 $\mathcal{V}_1$ 为另一代数簇 $\mathcal{V}_2$ 的 *子代数簇*, 记为 $\mathcal{V}_1 \subset \mathcal{V}_2$, 如果 $\mathcal{V}_1$ 中的所有点都在 $\mathcal{V}_2$ 中. 若 $\mathcal{V}_1 \subset \mathcal{V}_2$ 且 $\mathcal{V}_1 \neq \mathcal{V}_2$, 则称 $\mathcal{V}_1$ 为 $\mathcal{V}_2$ 的 *真* 子代数簇.

定义 6.1.4 称代数簇 $\mathcal{V} \subset \mathbf{A}^n_{\tilde{\mathcal{K}}}$ 为 *不可约的*, 如果不能将 $\mathcal{V}$ 表示为它的两个真子代数簇 $\mathcal{V}_1$ 和 $\mathcal{V}_2$ 的并. 此时，也称 $\mathcal{V}$ 的定义多项式组为 *不可约的*.

称 $\mathcal{K}$ 的某一扩域上的代数簇 $\mathcal{V}$ 中的任意一点 $\boldsymbol{\xi}$ 为 $\mathcal{V}$ 的 *一般点*, 如果 $\mathcal{K}[\boldsymbol{x}]$ 中每个在 $\boldsymbol{\xi}$ 处为零的多项式在 $\mathcal{V}$ 上都恒为零.

定义 6.1.5 设代数簇 $\mathcal{V} \subset \mathbf{A}^n_{\mathcal{K}}$ 由多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 所定义，且 $\mathcal{V} \neq \emptyset$. $\mathbb{P}$ 的维数也称为 $\mathcal{V}$ 或 $\mathrm{Zero}(\mathbb{P})$ 的 *维数*. 用符号表示，即

$$\mathrm{Dim}(\mathcal{V}) = \mathrm{Dim}(\mathrm{Zero}(\mathbb{P})) = \mathrm{Dim}(\mathbb{P}).$$

非空代数簇的维数是刻画代数簇的基本不变量之一. 这里给出的定义与标准代数几何论著中的定义是等价的. 这一点可从 (下节中予以证明的) 如下事实看出. 从 $\mathbb{P}$ 的不可约三角序列 Ψ 中的每个不可约三角列 $\mathbb{T}$, 我们可以构造一个不可约代数簇 $\mathcal{V}_{\mathbb{T}} \subset \mathcal{V} = \mathrm{Zero}(\mathbb{P})$, 使得 $\mathbb{T}$ 的每个一般零点都是 $\mathcal{V}_{\mathbb{T}}$ 的一般点，且

$$\mathcal{V} = \bigcup_{\mathbb{T}\in\Psi} \mathcal{V}_{\mathbb{T}}.$$

于是 $\mathrm{Dim}(\mathcal{V}_{\mathbb{T}}) = \dim(\mathbb{T})$ 与代数几何中定义的 $\mathcal{V}_{\mathbb{T}}$ 的维数相吻合，因而 $\mathrm{Dim}(\mathcal{V}) = \mathrm{Dim}(\mathbb{P})$ 也是如此.

定义 6.1.6 代数簇 $\mathcal{V} \subset \mathbf{A}^n_{\mathcal{K}}$ 的一个 *不可约分支* 是 $\mathcal{V}$ 的一不可约子代数簇 $\mathcal{W}$. $\mathcal{W}$ 的任意定义多项式组也称为 $\mathcal{V}$ 的定义多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 的 *不可约分支*. $\mathcal{W}$ 称为是 *无赘的*, 如果它不包含于 $\mathcal{V}$ 的另一不可约子代数簇.

注意：代数几何中所说的不可约分支通常是指无赘不可约分支. 以下我们重温代数几何中有关维数的若干结果 (如见 [29] 第 7, 8 和 48 页). 其中有些结果也容易用三角序列来证明. 我们略去这些证明，有兴趣的读者可将其作为练习.

命题 6.1.7 不可约多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 的维数为 $n-1$ 当且仅当 $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(P)$, 这里 P 为 $\mathcal{K}$ 上的不可约、非常数多项式.

命题 6.1.8 设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的不可约多项式组，而 P 为任一多项式，且 $\mathrm{Zero}(\mathbb{P}) \not\subset \mathrm{Zero}(P)$. 若 $\mathrm{Zero}(\mathbb{P} \cup \{P\}) \neq \emptyset$, 则 $\mathbb{P} \cup \{P\}$ 的所有无赘不可约分支都具有相同的维数 $\mathrm{Dim}(\mathbb{P}) - 1$, 因此它也是 $\mathbb{P} \cup \{P\}$ 的维数.

该命题的一个弱形式是: $\mathrm{Dim}(\mathbb{P}\cup\{P\}) < \mathrm{Dim}(\mathbb{P})$. 关于其证明，见 [96] (183 和 184 页).

命题 6.1.9 设 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 为任一多项式组，且 $\mathrm{Zero}(\mathbb{P}) \neq \emptyset$, 那么 $\mathbb{P}$ 的每个无赘不可约分支的维数都 $\geq n - |\mathbb{P}|$. 特别有

$$\mathrm{Dim}(\mathbb{P}) \geq n - |\mathbb{P}|.$$

命题 6.1.10 (仿射维数定理) 设 $\mathbb{P}_1, \mathbb{P}_2 \subset \mathcal{K}[\boldsymbol{x}]$ 是维数分别为 s_1, s_2 的不可约多项式组，那么 $\mathbb{P}_1 \cup \mathbb{P}_2$ 的每个无赘不可约分支的维数都 $\geq s_1 + s_2 - n$，因而 $\mathbb{P}_1 \cup \mathbb{P}_2$ 的维数也是如此.

定理 6.1.11 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的正则列，P 为任一使得对任意 $\boldsymbol{\xi} \in \mathrm{RegZero}(\mathbb{T})$ 都有 $P(\boldsymbol{\xi}) \neq 0$ 的多项式，而 Ψ 为 $[\mathbb{T} \cup \{P\}, \mathrm{ini}(\mathbb{T})]$ 的三角序列，那么对每个 $\mathfrak{T} \in \Psi$，或者 $\mathfrak{T}$ 是不完美的，或者 $\dim(\mathfrak{T}) < \dim(\mathbb{T})$.

证 依命题 3.2.6, $R = \mathrm{res}(P, \mathbb{T})$ 是一个不含 $\mathbb{T}$ 的依量的非零多项式. 设 $\mathbb{T}_1, \cdots, \mathbb{T}_e$ 为 $\{R\}$ 的特征序列，那么可将每个 $\mathbb{T} \cup \mathbb{T}_i$ 排为三角列 $\mathbb{T}_i^*$. 或者 $\mathbb{T}_i^*$ 是不完美的，或者 $\dim(\mathbb{T}_i^*) \leq \dim(\mathbb{T}) - 1 < \dim(\mathbb{T})$. 另一方面，

$$\mathrm{Zero}(\mathbb{T} \cup \{P\}/\mathrm{ini}(\mathbb{T})) \subset \mathrm{Zero}(\mathbb{T} \cup \{R\}/\mathrm{ini}(\mathbb{T})) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i^*/\mathrm{ini}(\mathbb{T}_i^*)).$$

如果 $e = 0$ (在 $R \in \mathcal{K}$ 时) 或者所有 $\mathbb{T}_i^*$ 都是不完美的，那么 $\mathrm{Zero}(\mathbb{T} \cup \{P\}/\mathrm{ini}(\mathbb{T})) = \emptyset$, 且每个 $\mathfrak{T} \in \Psi$ 都是不完美的. 所以对每个 $\mathfrak{T} \in \Psi$, 或者 $\mathfrak{T}$ 是不完美的或者 $\dim(\mathfrak{T}) < \dim(\mathbb{T})$. 定理获证. □

该定理在 $\mathbb{T}$ 不可约且 $\mathrm{prem}(P, \mathbb{T}) \neq 0$ 时也成立. 这是因为任意不可约三角列 $\mathbb{T}$ 都是正则的，且对 $\mathbb{T}$ 的每个一般零点 $\boldsymbol{\xi}$ 都有 $P(\boldsymbol{\xi}) \neq 0$ 当且仅当 $\mathrm{prem}(P, \mathbb{T}) \neq 0$ (见引理 4.5.1). 在上述定理中，如果 Ψ 为 $[\mathbb{T} \cup \{P\}, \mathbb{U}]$ 的三角序列，这里 $\mathbb{U}$ 为任一使得 $[\mathbb{T}, \mathbb{U}]$ 构成三角系统的多项式组，则结论仍然成立.

6.2 代数簇的分解

将代数簇分解为不可约或等维分支是经典代数几何中的基本问题，并在现代几何工程中有诸多应用. 我们可以特别提及这些应用中的两点：其一是计算机辅助几何设计，此时欲将所考虑的几何对象分解为 较简单 的子对象；其二是几何定理机器证明，此时需要分解几何假设的构形以确定在哪些分支上几何定理成立.

鉴于代数簇与理想之间的关系，代数簇的分解将导致相应理想之根理想的分解，反之亦然. 因而在本节中我们将这两种分解混合起来介绍.

三角列的理想浸润

定义 6.2.1　设 $\mathfrak{I}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的理想，而 F 为多项式. $\mathfrak{I}$ 关于 F 的 *浸润* 为无限集合

$$\mathfrak{I}:F^{\infty}\triangleq\{P\in\mathcal{K}[\boldsymbol{x}]:\ F^{q}P\in\mathfrak{I}\ \text{对某一整数}\ q>0\ \text{成立}\}.$$

容易依定义验证 $\mathfrak{I}:F^{\infty}$ 为理想. 这一点也可以从如下引理看出.

引理 6.2.1　设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式组，F 为多项式，而 $\mathbb{P}^{*}=\mathbb{P}\cup\{zF-1\}$, 其中 z 为新变元，那么 $P\in\operatorname{Ideal}(\mathbb{P}^{*})\cap\mathcal{K}[\boldsymbol{x}]$ 当且仅当存在整数 $q>0$, 使得 $F^{q}P\in\operatorname{Ideal}(\mathbb{P})$.

证　设 $P\in\operatorname{Ideal}(\mathbb{P}^{*})\cap\mathcal{K}[\boldsymbol{x}]$, 则存在多项式 $Q_i,Q\in\mathcal{K}[\boldsymbol{x},z]$, 使得

$$P=\sum_{P_i\in\mathbb{P}}Q_iP_i+Q\,(zF-1).$$

上式中 z 任意，因此我们可以用 $1/F$ 来替换 z. 将所得的等式通分，我们可得如下形式的表达式:

$$F^{s}P=\sum_{P_i\in\mathbb{P}}Q_i^{*}P_i,$$

其中 $s\geq 0$ 为某一整数，$Q_i^{*}\in\mathcal{K}[\boldsymbol{x}]$ 为多项式. 由此即得 $F^{q}P\in\operatorname{Ideal}(\mathbb{P})$, 这里 $q=\max(s,1)>0$.

另一方面，若对某一整数 $q>0$ 有 $F^{q}P\in\operatorname{Ideal}(\mathbb{P})$, 则

$$(zF)^{q}P\in\operatorname{Ideal}(\mathbb{P}^{*})\subset\mathcal{K}[\boldsymbol{x},z].$$

所以

$$\begin{aligned}P&=(zF)^{q}P-[(zF)^{q}-1]\,P\\&=(zF)^{q}P-(zF-1)\left[(zF)^{q-1}+\cdots+1\right]P\in\operatorname{Ideal}(\mathbb{P}^{*}).\end{aligned}$$ □

下述引理与引理 6.2.1 平行，而且其证明也类似.

引理 6.2.2　设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式组，$F_1,\cdots,F_t$ 为 t 个多项式，而

$$\mathbb{P}^{*}=\mathbb{P}\cup\{z_iF_i-1:\ 1\leq i\leq t\},$$

其中 $z_1,\cdots,z_t$ 均为新变元，那么 $P\in\operatorname{Ideal}(\mathbb{P}^{*})\cap\mathcal{K}[\boldsymbol{x}]$ 当且仅当存在整数 $q_1>0,\cdots,q_t>0$, 使得 $F_1^{q_1}\cdots F_t^{q_t}P\in\operatorname{Ideal}(\mathbb{P})$.

证 设 $P \in \text{Ideal}(\mathbb{P}^\star) \cap \mathcal{K}[\boldsymbol{x}]$, 则存在多项式 $Q_i, H_j \in \mathcal{K}[\boldsymbol{x}, z_1, \cdots, z_t]$, 使得

$$P = \sum_{P_i \in \mathbb{P}} Q_i P_i + \sum_{j=1}^{t} H_j (z_j F_j - 1).$$

该等式对任意 $z_1, \cdots, z_t$ 成立, 因而对每个 j 可用 $1/F_j$ 替换 z_j. 将所得表达式通分 (并在必要时将其结果乘上 F_i), 我们有

$$F_1^{q_1} \cdots F_t^{q_t} P = \sum_{P_i \in \mathbb{P}} Q_i^* P_i \in \text{Ideal}(\mathbb{P}),$$

其中 $q_1 > 0, \cdots, q_t > 0$, $Q_i^* \in \mathcal{K}[\boldsymbol{x}]$.

反之, 假设对某些整数 $q_1 > 0, \cdots, q_t > 0$ 有 $F_1^{q_1} \cdots F_t^{q_t} P \in \text{Ideal}(\mathbb{P})$, 则

$$(z_1 F_1)^{q_1} \cdots (z_t F_t)^{q_t} P \in \text{Ideal}(\mathbb{P}^\star) \subset \mathcal{K}[\boldsymbol{x}, z_1, \cdots, z_t].$$

该表达式的左边可以写为

$$[(z_1 F_1 - 1) + 1]^{q_1} \cdots [(z_t F_t - 1) + 1]^{q_t} P = \sum_{i=1}^{t} R_i (z_i F_i - 1) + P,$$

这里 $R_i \in \mathcal{K}[\boldsymbol{x}, z_1, \cdots, z_t]$. 由此可得 $P \in \text{Ideal}(\mathbb{P}^\star) \cap \mathcal{K}[\boldsymbol{x}]$. 引理获证. □

引理 6.2.3 设 $\mathfrak{J}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中 $\mathbb{P}$ 生成的理想, 而 F 为多项式; $F_1, \cdots, F_t$ 为 F 的 t 个因子, 使得 $F_1 \cdots F_t \neq 0 \iff F \neq 0$;

$$\mathbb{P}^* = \mathbb{P} \cup \{zF - 1\}, \quad \mathbb{P}^\star = \mathbb{P} \cup \{z_i F_i - 1 : \ 1 \leq i \leq t\},$$

其中 $z, z_1, \cdots, z_t$ 为新变元; $\mathbb{G}^*, \mathbb{G}^\star$ 分别为 $\mathbb{P}^*$ 在 $\mathcal{K}[\boldsymbol{x}, z]$ 中和 $\mathbb{P}^\star$ 在 $\mathcal{K}[\boldsymbol{x}, z_1, \cdots, z_t]$ 中关于 $x_l \prec z$ 与 $x_l \prec z_j$ 所确定的纯字典序的格罗布讷基, 那么

$$\begin{aligned} \mathfrak{J} : F^\infty &= \text{Ideal}(\mathbb{P}^*) \cap \mathcal{K}[\boldsymbol{x}] = \text{Ideal}(\mathbb{G}^* \cap \mathcal{K}[\boldsymbol{x}]) \\ &= \text{Ideal}(\mathbb{P}^\star) \cap \mathcal{K}[\boldsymbol{x}] = \text{Ideal}(\mathbb{G}^\star \cap \mathcal{K}[\boldsymbol{x}]). \end{aligned}$$

证 第一个等式是引理 6.2.1 的推论. 右边的两个等式由格罗布讷基的消元性质可得 (见定理 5.3.5). 因此我们只需证明

$$\text{Ideal}(\mathbb{P}^*) \cap \mathcal{K}[\boldsymbol{x}] = \text{Ideal}(\mathbb{P}^\star) \cap \mathcal{K}[\boldsymbol{x}].$$

该等式将立即获证, 如果对任意 $P \in \mathcal{K}[\boldsymbol{x}]$, 存在整数 $q > 0$, 使得 $F^q P \in \mathfrak{J}$, 当且仅当存在整数 $q_1 > 0, \cdots, q_t > 0$, 使得 $F_1^{q_1} \cdots F_t^{q_t} P \in \mathfrak{J}$. 由于每个 F_i 都是 F 的因子而 $F_1 \cdots F_t \neq 0 \iff F \neq 0$, 以上要求显然满足. □

事实上，关于格罗布讷基的计算，任意使得 $x_1^{i_1}\cdots x_n^{i_n}\prec z$ 的容许项序都是可以的. 上述计算浸润基的技巧曾由多位学者独立提出 (见文献 [28, 17, 75]).

对于任意 $\mathfrak{I}:F^{\infty}$，还有另一种方法可以用来确定其有限基，该方法有可能实际上更有效. 它是通过计算商理想 $\mathfrak{I}:F^k$ 的基，其中 k 从 1 开始并逐一递增. 在 $\mathfrak{I}:F^k=\mathfrak{I}:F^{k+1}$ 对某一 k 成立时，我们得到 $\mathfrak{I}:F^{\infty}$ 的基；此时 $\mathfrak{I}:F^k=\mathfrak{I}:F^{\infty}$. 见定义 6.4.2, 引理 6.4.1 和著作 [21].

定义 6.2.2 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中任一三角列. 定义 $\mathbb{T}$ 的 *浸润* 为理想

$$\mathrm{sat}(\mathbb{T})\triangleq \mathrm{Ideal}(\mathbb{T}):J^{\infty},$$

式中 $J=\prod_{T\in\mathbb{T}}\mathrm{ini}(T)$.

设 $\mathbb{P}$ 为 $\mathrm{sat}(\mathbb{T})$ 的有限基，下面的关系式显然成立：

$$\mathrm{Ideal}(\mathbb{T})\subset \mathrm{sat}(\mathbb{T})=\mathrm{Ideal}(\mathbb{P}).$$

定义 6.2.3 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中任一三角列. 定义 $\mathbb{T}$ 的 p *浸润* 为无限集合

$$\text{p-sat}(\mathbb{T})\triangleq\{P\in\mathcal{K}[\boldsymbol{x}]:\ \mathrm{prem}(P,\mathbb{T})=0\}.$$

定理 6.2.4 对任意正则列 $\mathbb{T}\subset\mathcal{K}[\boldsymbol{x}]$, $\mathrm{sat}(\mathbb{T})=\text{p-sat}(\mathbb{T})$.

证 设 $P\in\text{p-sat}(\mathbb{T})$，且命 $J=\prod_{T\in\mathbb{T}}\mathrm{ini}(T)$，则 $\mathrm{prem}(P,\mathbb{T})=0$. 由余式公式 (2.1.2)，存在整数 $q>0$，使得 $J^qP\in\mathrm{Ideal}(\mathbb{T})$. 于是由定义 6.2.1 和 6.2.2 可知 $P\in\mathrm{sat}(\mathbb{T})$.

欲证其反向，将 $\mathbb{T}$ 写为 $\mathbb{T}=[T_1,\cdots,T_r]$，并令

$$I_i=\mathrm{ini}(T_i),\quad J_i=I_1\cdots I_i,\quad 1\le i\le r,$$

那么，对任意 $P\in\mathrm{sat}(\mathbb{T})$，存在整数 $q>0$ 与多项式 $Q_i\in\mathcal{K}[\boldsymbol{x}]$，使得

$$J_r^qP=Q_1T_1+\cdots+Q_rT_r. \tag{6.2.1}$$

现在我们对 r 使用归纳法证明如下断言：

(A) 如果 $P\in\mathrm{sat}(\mathbb{T})$ 对 $\mathbb{T}$ 是约化的，则 $P\equiv 0$.

若 $r=1$，则 (6.2.1) 成为 $J_1^qP=Q_1T_1$. 这只有在 $Q_1\equiv 0$ 时才可能. 原因是 P 对 T_1 约化，因而 $\mathrm{ldeg}(T_1)>\deg(P,\mathrm{lv}(T_1))$. 于是 $P\equiv 0$.

假设 (A) 对任意长度 $< r$ 的正则列 $\mathbb{T}$ 成立. 今证其对 $r = |\mathbb{T}| > 1$ 亦然. 为此, 置

$$x_{p_r} = \mathrm{lv}(T_r),\quad d_r = \mathrm{ldeg}(T_r),\quad m = \deg(Q_r, x_{p_r}) \geq -1.$$

在 $Q_r \neq 0$ 的情形, 考虑系数

$$F_r = \mathrm{lc}(Q_r, x_{p_r}),\quad F_i = \mathrm{coef}(Q_i, x_{p_r}^{m+d_r}),\ 1 \leq i \leq r-1.$$

由于 $T_1, \cdots, T_{r-1}$ 不含有 x_{p_r} 而 P 对 T_r 约化, 故有

$$\sum_{i=1}^{r-1} F_i T_i + F_r I_r = \mathrm{coef}\left(\sum_{i=1}^{r} Q_i T_i, x_{p_r}^{m+d_r}\right) = \mathrm{coef}(J_r^q P, x_{p_r}^{m+d_r}) = 0. \quad (6.2.2)$$

将 (6.2.1) 式乘上 I_r 并使用 (6.2.2), 我们有

$$J_r^q I_r P = Q_1' T_1 + \cdots + Q_r' T_r, \quad (6.2.3)$$

这里

$$Q_i' = I_r Q_i - T_r F_i x_{p_r}^m,\ 1 \leq i \leq r-1,\quad Q_r' = I_r\,\mathrm{red}(Q_r, x_{p_r}).$$

(6.2.3) 与 (6.2.1) 式的右边形式相同, 而 $\deg(Q_r', x_{p_r}) < m = \deg(Q_r, x_{p_r})$. 若 $Q_r' \neq 0$, 则按同样方式进行可得

$$J_r^q I_r^2 P = Q_1'' T_1 + \cdots + Q_r'' T_r,$$

使得 $\deg(Q_r'', x_{p_r}) < \deg(Q_r', x_{p_r})$. 这一过程必定在某一时刻终止, 使得

$$J_{r-1}^q I_r^s P = Q_1^* T_1 + \cdots + Q_{r-1}^* T_{r-1} \quad (6.2.4)$$

对整数 $s \geq q$ 与多项式 $Q_i^* \in \mathcal{K}[\boldsymbol{x}]$ 成立.

因 $\mathbb{T}$ 正则, 依引理 3.2.5 与命题 3.2.6, 存在多项式 $H, H_i \in \mathcal{K}[\boldsymbol{x}]$, 使得

$$H I_r^s + H_1 T_1 + \cdots + H_{r-1} T_{r-1} = S = \mathrm{res}(I_r^s, \mathbb{T}^{\{r-1\}}) \neq 0. \quad (6.2.5)$$

将 (6.2.4) 式乘上 H 并使用 (6.2.5), 我们得

$$J_{r-1}^q S P = \bar{Q}_1 T_1 + \cdots + \bar{Q}_{r-1} T_{r-1},$$

其中 $\bar{Q}_i = HQ_i^* + J_{r-1}^q H_i P,\ 1 \le i \le r-1$. 于是 $SP \in \mathrm{sat}(\mathbb{T}^{\{r-1\}})$. 因 S 不含有 $\mathbb{T}$ 的依量, 故 SP 对 $\mathbb{T}^{\{r-1\}}$ 是约化的. 依据归纳假设, $SP \equiv 0$; 因此 $P \equiv 0$. 断言 (A) 获证.

为了完成定理 6.2.4 的证明, 考虑任意 $P \in \mathrm{sat}(\mathbb{T})$, 并命 $R = \mathrm{prem}(P, \mathbb{T})$; R 对 $\mathbb{T}$ 是约化的. 因为对每个 i 显然有 $T_i \in \mathrm{sat}(\mathbb{T})$, 故由伪余公式可知 $R \in \mathrm{sat}(\mathbb{T})$. 按照上面的断言 (A), $R \equiv 0$. 所以 $P \in \text{p-sat}(\mathbb{T})$. □

而且可以证明, $\mathrm{sat}(\mathbb{T}) = \text{p-sat}(\mathbb{T})$ 也是任意三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$ 为正则列的充分条件 (见 [2]). 下面的结果是定理 6.2.4 的直接推论.

推论 6.2.5 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任意正则列, 而 $\mathbb{P}$ 为 $\mathrm{sat}(\mathbb{T})$ 的有限基, 则 $\mathbb{T}$ 为 $\mathbb{P}$ 的 W 特征列.

事实上, 有一个比推论 6.2.5 更强的结果: 任意约化正则列 $\mathbb{T}$ 都是理想 $\mathrm{sat}(\mathbb{T})$ (在里特意义下) 的特征列 (见 [57] 第 174 至 176 页与 [62] 第 4 和 5 页).

对任意不可约三角列 $\mathbb{T}$, 定理 6.2.14 断言 $\mathrm{sat}(\mathbb{T})$ 为素理想. 对任意 $F \in \mathcal{K}[\boldsymbol{x}]$, 若 $\mathrm{prem}(F, \mathbb{T}) \ne 0$, 则按照定理 6.2.4 有 $F \notin \mathrm{sat}(\mathbb{T})$, 因此依据定义有 $\mathrm{sat}(\mathbb{T}) : F^\infty = \mathrm{sat}(\mathbb{T})$. 下述引理将这一结果推广到正则列.

引理 6.2.6 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的正则列, 而 F 为任一多项式. 若 $\mathrm{res}(F, \mathbb{T}) \ne 0$, 则 $\mathrm{sat}(\mathbb{T}) : F^\infty = \mathrm{sat}(\mathbb{T})$.

证 显然, $\mathrm{sat}(\mathbb{T}) \subset \mathrm{sat}(\mathbb{T}) : F^\infty$. 欲证其反方向, 命 $R = \mathrm{res}(F, \mathbb{T})$, 并设 $\mathbb{T}$ 形如 (3.2.1). 那么 $R \ne 0$, 且 $R \in \mathcal{K}[\boldsymbol{u}]$. 由引理 3.2.5, 存在多项式 $Q \in \mathcal{K}[\boldsymbol{u}, y_1, \cdots, y_r]$, 使得 $QF - R \in \mathrm{Ideal}(\mathbb{T}) \subset \mathrm{sat}(\mathbb{T})$. 现考虑任意 $P \in \mathrm{sat}(\mathbb{T}) : F^\infty$. 依据定义, 存在整数 $q > 0$, 使得 $F^q P \in \mathrm{sat}(\mathbb{T})$. 由此可得

$$R^q P = Q^q F^q P - (QF - R)[(QF)^{q-1} + \cdots + R^{q-1}]P \in \mathrm{sat}(\mathbb{T}).$$

令 $H = \mathrm{prem}(P, \mathbb{T})$, 则由伪余公式可见 $R^q H \in \mathrm{sat}(\mathbb{T})$. 依定理 6.2.4, $R^q H \in \text{p-sat}(\mathbb{T})$, 因此 $\mathrm{prem}(R^q H, \mathbb{T}) = 0$. 由于 $R \in \mathcal{K}[\boldsymbol{u}]$ 不含有 $\mathbb{T}$ 的依量, 而 H 对 $\mathbb{T}$ 约化, 故有 $R^q H = \mathrm{prem}(R^q H, \mathbb{T}) = 0$. 所以 $\mathrm{prem}(P, \mathbb{T}) = H = 0$, 因而 $P \in \text{p-sat}(\mathbb{T}) = \mathrm{sat}(\mathbb{T})$. 证毕. □

命题 6.2.7 设 $[\mathbb{T}, \mathbb{U}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的正则系统, 而 $V = \prod_{U \in \mathbb{U}} U$, 则

$$\mathrm{Ideal}(\mathbb{T}) : V^\infty = \mathrm{sat}(\mathbb{T}). \tag{6.2.6}$$

证 命 $\mathfrak{I} = \mathrm{Ideal}(\mathbb{T})$, $J = \prod_{T\in\mathbb{T}} \mathrm{ini}(T)$. 因 $[\mathbb{T}, \mathbb{U}]$ 正则, 故 $\mathrm{res}(V, \mathbb{T}) \neq 0$. 由引理 6.2.6 和定义 6.2.1 可知

$$\mathrm{sat}(\mathbb{T}) = \mathrm{sat}(\mathbb{T}) : V^{\infty} = (\mathfrak{I} : J^{\infty}) : V^{\infty} = \mathfrak{I} : (JV)^{\infty}.$$

由于对任意 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}/V)$ 都有 $J(\bar{\boldsymbol{x}}) \neq 0$, 所以 $\mathrm{Zero}(\mathbb{T} \cup \{J\}) \subset \mathrm{Zero}(V)$. 根据希尔伯特零点定理, 存在整数 $s > 0$ 与多项式 $Q \in \mathcal{K}[\boldsymbol{x}]$, 使得 $V^s - QJ \in \mathfrak{I}$. 考虑任意 $P \in \mathfrak{I} : (JV)^{\infty}$, 则存在整数 $q > 0$, 使得 $(JV)^q P \in \mathfrak{I}$. 于是有

$$V^{(s+1)q}P = V^q(V^s - QJ)[V^{s(q-1)} + \cdots + (QJ)^{q-1}]P + Q^q(JV)^q P \in \mathfrak{I}.$$

因此 $P \in \mathfrak{I} : V^{\infty}$.

另一方面, 依据定义有 $\mathfrak{I} : V^{\infty} \subset \mathfrak{I} : (JV)^{\infty}$. 因而,

$$\mathrm{sat}(\mathbb{T}) = \mathfrak{I} : (JV)^{\infty} = \mathfrak{I} : V^{\infty}$$

获证. □

可用命题 6.2.7 给出定理 3.2.10 的另一简单证明 (见 [91]). 作为 (6.2.6) 的推论, 我们有

$$\mathrm{Zero}(\mathrm{Ideal}(\mathbb{T}) : V^{\infty}) = \mathrm{Zero}(\mathrm{sat}(\mathbb{T})).$$

非混合分解

零点分解 (2.2.6) 提供了 $\mathbb{P}$ 所定义的代数簇 $\mathcal{V}$ 用 $\mathbb{C}_i$ 决定的子代数簇的一种表示. 可是, 每个 $\mathrm{Zero}(\mathbb{C}_i/\mathbb{I}_i)$ 并不一定是代数簇, 而是 *拟代数簇*. 以下, 我们将看到如何通过从每个 $\mathbb{C}_i$ 确定一组有限多个多项式来获得相应的代数簇分解.

定理 6.2.8 设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的非空多项式组, 而 $\mathbb{T}_1, \cdots, \mathbb{T}_e$ 为 $\mathbb{P}$ 的 (弱) 特征序列或正则序列, 则

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathrm{sat}(\mathbb{T}_i)). \qquad (6.2.7)$$

证 如果 $\mathbb{T}_1, \cdots, \mathbb{T}_e$ 为 $\mathbb{P}$ 的 (弱) 特征序列, 那么对每个 i 都有 $\mathrm{prem}(\mathbb{P}, \mathbb{T}_i) = \{0\}$; 否则, 由定理 3.2.12 (a), 存在整数 $d > 0$, 使得 $\mathrm{prem}(P^d, \mathbb{T}_i) = 0$ 对所有 $P \in \mathbb{P}$ 和 $1 \leq i \leq e$ 成立. 无论哪种情形, 由伪余公式都能得出 $\mathrm{Zero}(\mathrm{sat}(\mathbb{T}_i)) \subset \mathrm{Zero}(\mathbb{P})$.

现命 $J_i = \prod_{T\in\mathbb{T}_i} \mathrm{ini}(T)$, $1 \le i \le e$. 根据定义和定理 3.2.12 (c), 我们有

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/J_i).$$

所以, 对任意 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{P})$ 都存在 i, 使得 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathbb{T}_i/J_i)$. 设 P 为 $\mathrm{sat}(\mathbb{T}_i)$ 中任一多项式, 则存在整数 $q > 0$, 使得 $J_i^q P \in \mathrm{Ideal}(\mathbb{T}_i)$. 由此可见 $J_i(\bar{\boldsymbol{x}})^q P(\bar{\boldsymbol{x}}) = 0$. 因 $J_i(\bar{\boldsymbol{x}}) \neq 0$, 故 $P(\bar{\boldsymbol{x}}) \neq 0$. 所以 $\bar{\boldsymbol{x}} \in \mathrm{Zero}(\mathrm{sat}(\mathbb{T}_i))$. 定理获证. □

周咸青和高小山 [16] 用下述结果为抹去分解 (6.2.7) 中某些多余子代数簇 —— 而未计算其定义多项式组 —— 提供了一条实用的准则.

引理 6.2.9 设 $\mathbb{P}$ 和 $\mathbb{T}_i$ 与定理 6.2.8 中相同. 若 $|\mathbb{T}_j| > |\mathbb{P}|$, 则

$$\mathrm{Zero}(\mathrm{sat}(\mathbb{T}_j)) \subset \bigcup_{\substack{1\le i\le e\\ i\neq j}} \mathrm{Zero}(\mathrm{sat}(\mathbb{T}_i)),$$

因此 $\mathrm{Zero}(\mathrm{sat}(\mathbb{T}_j))$ 可从分解 (6.2.7) 中抹去.

证 因 $|\mathbb{T}_j| > |\mathbb{P}|$, 故 $\dim(\mathbb{T}_j) < n - |\mathbb{P}|$. 依命题 6.1.9 和定理 6.2.10, $\mathrm{Zero}(\mathrm{sat}(\mathbb{T}_j))$ 为 $\mathrm{Zero}(\mathbb{P})$ 的多余分支. □

定义 6.2.4 一个代数簇称为是 *非混合的* 或 *等维的*, 如果它的所有无赘不可约分支都具有相同的维数.

下述定理归功于高小山和周咸青 [26].

定理 6.2.10 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任意三角列. 如果 $\mathbb{T}$ 是不完美的, 则 $\mathrm{sat}(\mathbb{T}) = \mathcal{K}[\boldsymbol{x}]$; 如果 $\mathbb{T}$ 是完美的, 则 $\mathrm{Zero}(\mathrm{sat}(\mathbb{T}))$ 是维数为 $n - |\mathbb{T}|$ 的非混合代数簇.

证 命 $J = \prod_{T\in\mathbb{T}} \mathrm{ini}(T)$. 若 $\mathbb{T}$ 是不完美的, 则 $\mathrm{Zero}(\mathbb{T}) \subset \mathrm{Zero}(J)$. 依定理 1.6.3, 存在整数 $q > 0$, 使得 $J^q \in \mathrm{Ideal}(\mathbb{T})$. 于是对任意 $P \in \mathcal{K}[\boldsymbol{x}]$ 有 $J^q P \in \mathrm{Ideal}(\mathbb{T})$. 因此任意 $P \in \mathcal{K}[\boldsymbol{x}]$ 都属于 $\mathrm{sat}(\mathbb{T})$, 故 $\mathrm{sat}(\mathbb{T}) = \mathcal{K}[\boldsymbol{x}]$.

现假定 $\mathbb{T}$ 是完美的, 并设 $\mathbb{C}_1, \cdots, \mathbb{C}_e$ 为 $\mathbb{T}$ 的不可约特征序列. 置

$$\Theta = \{i\colon\ |\mathbb{C}_i| \le |\mathbb{T}|, 1 \le i \le e\},\quad \Theta^* = \{i \in \Theta\colon\ \mathrm{prem}(J, \mathbb{C}_i) \neq 0\}.$$

根据定理 6.2.8 和引理 6.2.9, 我们有

$$\mathrm{Zero}(\mathbb{T}) = \bigcup_{i\in\Theta} \mathrm{Zero}(\mathrm{sat}(\mathbb{C}_i)). \tag{6.2.8}$$

依推论 6.1.2, 又有

$$\max_{i\in\Theta^*} \dim(\mathbb{C}_i) = \dim(\mathbb{T}) = n - |\mathbb{T}|.$$

所以 $\Theta^* \neq \emptyset$, 而 $\dim(\mathbb{C}_i) = \dim(\mathbb{T})$ 对所有 $i \in \Theta^*$ 成立. 由 (6.2.8) 可见

$$\mathrm{Zero}(\mathbb{T}/J) = \bigcup_{i\in\Theta^*} \mathrm{Zero}(\mathrm{sat}(\mathbb{C}_i)/J).$$

因此

$$\mathrm{Zero}(\mathrm{sat}(\mathbb{T})) = \bigcup_{i\in\Theta^*} \mathrm{Zero}(\mathrm{sat}(\mathbb{C}_i) : J^\infty).$$

现固定 $i \in \Theta^*$. 因 $\mathbb{C}_i$ 不可约且 $\mathrm{prem}(J, \mathbb{C}_i) \neq 0$, 故依引理 6.2.6 (或该引理之前的说明) 有 $\mathrm{sat}(\mathbb{C}_i) : J^\infty = \mathrm{sat}(\mathbb{C}_i)$. 注意, 对每个 $i \in \Theta^*$, $\mathrm{Zero}(\mathrm{sat}(\mathbb{C}_i))$ 的维数都是 $n - |\mathbb{T}|$. 因而 $\mathrm{Zero}(\mathrm{sat}(\mathbb{T}))$ 是非混合的, 其维数为 $n - |\mathbb{T}|$. 如所欲证. □

记住, 任意正则、简单或不可约三角列 $\mathbb{T}$ 都是完美的, 所以 $\mathrm{sat}(\mathbb{T}) = \text{p-sat}(\mathbb{T})$, 其代数簇是非混合的, 且维数为 $n - |\mathbb{T}|$.

在分解 (6.2.7) 中, 对每个 i 设 $\mathbb{P}_i$ 为 $\mathrm{sat}(\mathbb{T}_i)$ 的有限基, 它可以按照引理 6.2.3 通过计算格罗布讷基而求得. 若 $\mathrm{sat}(\mathbb{T}_i) = \mathcal{K}[\boldsymbol{x}]$, 则常数 1 属于 $\mathbb{P}_i$ (的约化格罗布讷基). 假定已将这样的 $\mathbb{P}_i$ 抹去. 因此我们得到如下形式的代数簇分解:

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{P}_i). \tag{6.2.9}$$

依定理 6.2.10, 每个 $\mathbb{P}_i$ 都定义一非混合代数簇.

令 $\mathcal{V}_i = \mathrm{Zero}(\mathbb{P}_i)$, 则分解 (6.2.9) 可重写为

$$\mathcal{V} = \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_e. \tag{6.2.10}$$

这一分解不一定是不可缩的, 即某一代数簇 $\mathbb{P}_i$ 可能是另一代数簇的子簇. 使用引理 6.2.9, 容易抹去一些多余的子代数簇. 下述引理指出如何抹去一些其他的多余分支.

引理 6.2.11　设 $\mathbb{G}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的格罗布讷基，而 $\mathbb{P}$ 为任一多项式组. 如果 $\mathbb{P}$ 中所有多项式对 $\mathbb{G}$ 的余式都为 0, 则 $\mathrm{Zero}(\mathbb{G}) \subset \mathrm{Zero}(\mathbb{P})$.

证　因为 $\mathbb{P}$ 中所有多项式对 $\mathbb{G}$ 的余式都为 0, 所以 $\mathrm{Ideal}(\mathbb{P}) \subset \mathrm{Ideal}(\mathbb{G})$. 因此 $\mathrm{Zero}(\mathbb{G}) \subset \mathrm{Zero}(\mathbb{P})$. □

以上介绍的将代数簇分解为非混合分支的方法可以写成下面的算法.

算法 UnmVarDec: $\Psi \leftarrow \mathrm{UnmVarDec}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算有限多个多项式组 $\mathbb{P}_1, \cdots, \mathbb{P}_e$ 构成的集合 Ψ, 使得分解 (6.2.9) 成立，并且每个 $\mathbb{P}_i$ 都定义一非混合代数簇.

U1. 计算 $\Phi \leftarrow \mathrm{CharSer}(\mathbb{P})$, 且命 $\Psi \leftarrow \emptyset$.

U2. 重复下列步骤直至 $\Phi = \emptyset$:

- **U2.1.** 设 $\mathbb{C}$ 为 Φ 中的元素，且命 $\Phi \leftarrow \Phi \setminus \{\mathbb{C}\}$. 若 $|\mathbb{C}| > |\mathbb{P}|$, 则转至 U2.
- **U2.2.** 按引理 6.2.3 计算 $\mathrm{sat}(\mathbb{C})$ 的有限基，设该有限基为一格罗布讷基 $\mathbb{G}$, 且命 $\Psi \leftarrow \Psi \cup \{\mathbb{G}\}$.

U3. 只要 $\exists\, \mathbb{G}, \mathbb{G}^* \in \Psi$ 使 $\mathrm{rem}(\mathbb{G}, \mathbb{G}^*) = \{0\}$ 就一直执行:

$$\text{命 } \Psi \leftarrow \Psi \setminus \{\mathbb{G}^*\}.$$

该算法的终止性是显而易见的. 引理 6.2.3 和定理 6.2.10 保证了代数簇分解 (6.2.9) 的正确性以及每个 $\mathrm{Zero}(\mathbb{P}_i)$ 的非混合性.

由算法 UnmVarDec 计算的非混合分解 (6.2.9) 不一定是不可缩的. 要想去掉 *所有* 多余分支则需要额外的计算. 对于任一正则列 $\mathbb{T}$, $\mathrm{sat}(\mathbb{T})$ 不一定是根理想; 但它在 $\mathbb{T}$ 为简单列时一定是.

定理 6.2.12　对任意简单列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$, $\mathrm{p\text{-}sat}(\mathbb{T})$ 为根理想.

证　设 $P^q \in \mathrm{p\text{-}sat}(\mathbb{T})$, 则

$$\mathrm{Zero}(\mathbb{T}/\mathbb{I}) \subset \mathrm{Zero}(P^q) = \mathrm{Zero}(P),$$

于是依推论 3.4.5 有 $\mathrm{prem}(P, \mathbb{T}) = 0$. 所以 $P \in \mathrm{p\text{-}sat}(\mathbb{T})$, 因此 $\mathrm{p\text{-}sat}(\mathbb{T})$ 是根理想. □

由此可见，如果 UnmVarDec 步骤 U1 中的 Φ 是由算法 SimSer 计算的 $\mathbb{P}$ 的简单序列，那么对每个 $\mathbb{P}_i \in \Psi$, $\mathfrak{I}_i = \mathrm{Ideal}(\mathbb{P}_i)$ 都为根理想. 这就给出了下面的理想分解：

$$\sqrt{\mathfrak{I}} = \bigcap_{i=1}^{e} \mathfrak{I}_i,$$

这里 $\mathfrak{I} = \mathrm{Ideal}(\mathbb{P})$, 而每个 $\mathfrak{I}_i$ 都是非混合的根理想.

通过检查格罗布讷基之间的包含关系来抹去多余的子代数簇有一个缺陷，那就是一个分支只有在其相应的格罗布讷基已经求出之后才能被抹去. 下述引理提供了抹去多余分支的另一准则.

引理 6.2.13 设 $\mathbb{T}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的正则列，而 $\mathbb{P}$ 为 $\mathrm{sat}(\mathbb{T})$ 的有限基. 若 $\mathbb{P}^*$ 是使得 $\mathrm{prem}(\mathbb{P}^*, \mathbb{T}) = \{0\}$ 的多项式组，则 $\mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(\mathbb{P}^*)$.

证 因 $\mathbb{T}$ 正则而 $\mathrm{prem}(\mathbb{P}^*, \mathbb{T}) = \{0\}$, 故 $\mathbb{P}^* \subset \text{p-sat}(\mathbb{T}) = \mathrm{sat}(\mathbb{T})$. 因此

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathrm{sat}(\mathbb{T})) \subset \mathrm{Zero}(\mathbb{P}^*).$$

□

使用定理 6.2.12 和引理 6.2.13, 我们可以将算法 UnmVarDec 修改如下.

算法 UnmRadIdeDec: $\Psi \leftarrow \mathrm{UnmRadIdeDec}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算有限多个多项式组 $\mathbb{P}_1, \cdots, \mathbb{P}_e$ 构成的集合 Ψ, 使得分解 (6.2.9) 成立，并且每个 $\mathbb{P}_i$ 都生成一非混合的根理想.

U1. 计算 $\Phi \leftarrow \mathrm{SimSer}(\mathbb{P})$, 且命

$$\Phi \leftarrow \{\mathbb{T}\colon\ |\mathbb{T}| \leq |\mathbb{P}|, [\mathbb{T}, \tilde{\mathbb{T}}] \in \Phi\}, \quad \Psi \leftarrow \emptyset.$$

U2. 重复下列步骤直至 $\Phi = \emptyset$:

U2.1. 设 $\mathbb{T}$ 为 Φ 中维数最高的元素，且命 $\Phi \leftarrow \Phi \setminus \{\mathbb{T}\}$.

U2.2. 按引理 6.2.3 计算 $\mathrm{sat}(\mathbb{T})$ 的有限基，设所得的有限基为一格罗布讷基 $\mathbb{G}$, 且命 $\Psi \leftarrow \Psi \cup \{\mathbb{G}\}$.

U2.3. 只要 $\exists \mathbb{T}^* \in \Phi$ 使 $\mathrm{prem}(\mathbb{G}, \mathbb{T}^*) = \{0\}$ 就一直执行：

$$命\ \Phi \leftarrow \Phi \setminus \{\mathbb{T}^*\}.$$

U3. 只要 $\exists \mathbb{G}, \mathbb{G}^* \in \Psi$ 使 $\mathrm{rem}(\mathbb{G}, \mathbb{G}^*) = \{0\}$ 就一直执行：

命 $\Psi \leftarrow \Psi \setminus \{\mathbb{G}^*\}$.

一个代数簇 $\mathcal{V}_1$ 是另一代数簇 $\mathcal{V}_2$ 的真子簇只有在 $\mathrm{Dim}(\mathcal{V}_1) \leq \mathrm{Dim}(\mathcal{V}_2)$ 时才可能. 步骤 U2.1 中 $\mathbb{T}$ 的选取以及步骤 U2.3 中的检测使我们能在计算其定义多项式组之前抹去一些多余分支. 最后一步 U3 的目的是抹去那些包含其他与之有相同维数的根理想. 通过观察算法的步骤可知, 对 SimSer 计算的任意简单序列 Φ 应该不存在相同维数的 $\mathbb{G}, \mathbb{G}' \in \Psi$, 使得 $\mathrm{rem}(\mathbb{G}, \mathbb{G}') = \{0\}$, 即 $\mathrm{Ideal}(\mathbb{G}) \subset \mathrm{Ideal}(\mathbb{G}')$. 但这种包含关系对任意简单序列 Φ 则是可能的.

对任意给定生成元的理想 $\mathfrak{I}$, 算法 UnmRadIdeDec 加上理想交的计算提供了求根理想 $\sqrt{\mathfrak{I}}$ 之生成元的一种方法. 计算简单序列和格罗布讷基的算法从理论上来讲都不需要多项式因子分解, 因此计算非混合分解的算法也不需要.

不可约分解

现在我们考虑将任一多项式组定义的代数簇分解为不可约子代数簇. 这与 $\mathbb{P}$ 的非混合分解相仿, 附加条件是特征序列 Φ 不可约. 此时, 对 $\mathbb{C} \in \Phi$, $\mathrm{sat}(\mathbb{C})$ 的有限基定义一个不可约代数簇, 使得 $\mathbb{C}$ 的一般零点为其一般点.

定义 6.2.5　理想 $\mathfrak{I} \subset \mathcal{K}[\boldsymbol{x}]$ 称为是*素的*, 如果在 $F, G \in \mathcal{K}[\boldsymbol{x}]$, $FG \in \mathfrak{I}$ 时, 或者 $F \in \mathfrak{I}$, 或者 $G \in \mathfrak{I}$.

定理 6.2.14　对任意不可约三角列 $\mathbb{T} \subset \mathcal{K}[\boldsymbol{x}]$, $\mathrm{p\text{-}sat}(\mathbb{T})$ 都是素理想.

证　设 $\boldsymbol{\xi}$ 为 $\mathbb{T}$ 的一般零点, 则依引理 4.5.1, 对任意 $P \in \mathcal{K}[\boldsymbol{x}]$,

$$\mathrm{prem}(P, \mathbb{T}) = 0 \iff P(\boldsymbol{\xi}) = 0.$$

又设 $FG \in \mathrm{p\text{-}sat}(\mathbb{T})$, 则 $\mathrm{prem}(FG, \mathbb{T}) = 0$, 于是

$$F(\boldsymbol{\xi})G(\boldsymbol{\xi}) = 0.$$

因此或者 $F(\boldsymbol{\xi}) = 0$, 或者 $G(\boldsymbol{\xi}) = 0$, 即或者 $\mathrm{prem}(F, \mathbb{T}) = 0$, 或者 $\mathrm{prem}(G, \mathbb{T}) = 0$. 换言之, 或者 $F \in \mathrm{p\text{-}sat}(\mathbb{T})$, 或者 $G \in \mathrm{p\text{-}sat}(\mathbb{T})$. 所以 $\mathrm{p\text{-}sat}(\mathbb{T})$ 是素理想. □

在 $\mathrm{sat}(\mathbb{T}) = \mathrm{p\text{-}sat}(\mathbb{T})$ 为素理想时, 称其有限基为 $\mathbb{T}$ 的*素基*, 记作 $\mathrm{PB}(\mathbb{T})$, 那么 $\mathrm{PB}(\mathbb{T})$ 定义的代数簇应以 $\mathbb{T}$ 的一般零点为其一般点.

命题 6.2.15　设 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的不可约三角列, 且二者具有相同的一般零点, 则 $\mathrm{sat}(\mathbb{T}_1) = \mathrm{sat}(\mathbb{T}_2)$.

证 因为 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 都不可约且具有相同的一般零点，所以它们有相同的参量，并且依引理 4.5.1 有 $\text{prem}(\mathbb{T}_2,\mathbb{T}_1)=\text{prem}(\mathbb{T}_1,\mathbb{T}_2)=\{0\}$. 因此

$$\text{Ideal}(\mathbb{T}_2)\subset\text{sat}(\mathbb{T}_1),\quad \text{Ideal}(\mathbb{T}_1)\subset\text{sat}(\mathbb{T}_2).$$

考虑任一多项式 $P\in\mathcal{K}[\boldsymbol{x}]$. 若 $P\notin\text{sat}(\mathbb{T}_2)$, 则 $\text{prem}(P,\mathbb{T}_2)\neq 0$. 按照引理 3.2.5, 存在多项式 $Q\in\mathcal{K}[\boldsymbol{x}]$, 使得

$$QP-R\in\text{Ideal}(\mathbb{T}_2),$$

其中 $R=\text{res}(P,\mathbb{T}_2)$. 由此可知 $QP-R\in\text{sat}(\mathbb{T}_1)$. 因 $\text{prem}(R,\mathbb{T}_1)=R\neq 0$ (参阅引理 4.5.2), 故 $R\notin\text{sat}(\mathbb{T}_1)$. 所以 P 不能属于 $\text{sat}(\mathbb{T}_1)$. 这就证明了 $\text{sat}(\mathbb{T}_1)\subset\text{sat}(\mathbb{T}_2)$.

由于 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 是对等的，使用同样的论证可得 $\text{sat}(\mathbb{T}_2)\subset\text{sat}(\mathbb{T}_1)$. 证毕. □

命题 6.2.15 中的结论在 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 是具有相同正则零点的简单列时仍然成立. 其证明需要推论 3.4.5 的推广：对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意简单列 $\mathbb{T}$ 和多项式 P,

$$\text{RegZero}(\mathbb{T})\subset\text{Zero}(P)\iff\text{prem}(P,\mathbb{T})=0.$$

命题 6.2.16 设 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的三角列，二者具有相同的参量，且 $\mathbb{T}_2$ 是不可约的. 若 $\text{prem}(\mathbb{T}_2,\mathbb{T}_1)=\{0\}$, 则 $\mathbb{T}_1$ 也是不可约的，且与 $\mathbb{T}_2$ 有相同的一般零点，因此 $\text{sat}(\mathbb{T}_1)=\text{sat}(\mathbb{T}_2)$.

证 由于 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 具有相同的参量，所以可将它们写为

$$\mathbb{T}_i=[T_{i1}(\boldsymbol{u},y_1),\cdots,T_{ir}(\boldsymbol{u},y_1,\cdots,y_r)],\quad i=1,2.$$

又因 $\text{prem}(\mathbb{T}_2,\mathbb{T}_1)=\{0\}$, 故 $\text{prem}(T_{21},T_{11})=0$. 因此 T_{21} 的不可约性蕴涵着 T_{11} 在 $\mathcal{K}_0=\mathcal{K}(\boldsymbol{u})$ 上也不可约，并且 T_{11} 和 T_{21} 只相差一个 $\mathcal{K}_0$ 中的因子. 类似地， $\text{prem}(T_{22},[T_{11},T_{12}])=0$. 现在 T_{21} 在 $\mathcal{K}_1=\mathcal{K}_0(y_1)$ 上不可约，这里 y_1 的添加多项式为 T_{21} 或 T_{11}. 由伪余公式可知 T_{12} 在 $\mathcal{K}_1$ 上整除 T_{22}, 因此 T_{12} 与 T_{22} 只差一个 $\mathcal{K}_1$ 中的因子.

继续这一论证，我们将会看到： T_{1k} 和 T_{2k} 只相差代数扩域 $\mathcal{K}_{k-1}=\mathcal{K}_0(y_1,\cdots,y_{k-1})$ 中的一个因子，因此它们关于 y_k 在 $\mathcal{K}_{k-1}$ 中有相同的零点集，这里 $y_1,\cdots,y_{k-1}$ 的添加三角列为 $\mathbb{T}_1^{\{k-1\}}$ 或 $\mathbb{T}_2^{\{k-1\}}$, $1\leq k\leq r$. 所以 $\mathbb{T}_1$ 也是不可约的，且与 $\mathbb{T}_2$ 有相同的一般零点集. 根据命题 6.2.15, $\text{sat}(\mathbb{T}_1)=\text{sat}(\mathbb{T}_2)$. □

命题 6.2.16 推广了文献 [16] 中的一个结果；该文的作者也证明了如下命题.

命题 6.2.17　设 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的三角列，其中 $\mathbb{T}_1$ 不可约. 若 $\mathrm{prem}(\mathbb{T}_2,\mathbb{T}_1)=\{0\}$ 并且 $0\notin\mathrm{prem}(\mathrm{ini}(\mathbb{T}_2),\mathbb{T}_1)$, 则 $\mathrm{sat}(\mathbb{T}_2)\subset\mathrm{sat}(\mathbb{T}_1)$.

证　对任意 $P\in\mathrm{sat}(\mathbb{T}_2)$, 依据定义存在整数 $q>0$, 使得 $J_2^qP\in\mathrm{Ideal}(\mathbb{T}_2)$, 这里 $J_2=\prod_{T\in\mathbb{T}_2}\mathrm{ini}(T)$. 因 $\mathbb{T}_1$ 不可约且 $\mathrm{prem}(\mathbb{T}_2,\mathbb{T}_1)=\{0\}$, 故 $\mathrm{Ideal}(\mathbb{T}_2)\subset\mathrm{sat}(\mathbb{T}_1)$. 因此 $J_2^qP\in\mathrm{sat}(\mathbb{T}_1)$. 由于 $\mathrm{sat}(\mathbb{T}_1)$ 是素理想，而 $0\notin\mathrm{prem}(\mathrm{ini}(\mathbb{T}_2),\mathbb{T}_1)$ 蕴涵着 $J_2^q\notin\mathrm{sat}(\mathbb{T}_1)$, 我们有 $P\in\mathrm{sat}(\mathbb{T}_1)$. 所以 $\mathrm{sat}(\mathbb{T}_2)\subset\mathrm{sat}(\mathbb{T}_1)$.　□

根据定理 6.2.14, 要想确定 $\mathbb{T}$ 的素基，我们只需按引理 6.2.3 计算 $\mathbb{T}^*$ 的格罗布纳基以求得 $\mathrm{Ideal}(\mathbb{T}^*)\cap\mathcal{K}[\boldsymbol{x}]$ 的生成元.

设 (6.2.7) 中的每个 $\mathbb{T}_i$ 都是不可约的，那么我们有如下零点分解：

$$\mathrm{Zero}(\mathbb{P})=\bigcup_{i=1}^{e}\mathrm{Zero}(\mathrm{PB}(\mathbb{T}_i)).$$

现在，可通过格罗布纳基求出的每个 $\mathrm{PB}(\mathbb{T}_i)$ 都定义一不可约代数簇，因而我们完成了 $\mathbb{P}$ 所定义的代数簇 $\mathcal{V}$ 的不可约分解.

这样的分解不一定是极小的，但可以用命题 6.2.17 和引理 6.2.13 或 6.2.11 将所有多余的子代数簇去掉. 因此我们可以得到一个 极小 不可约分解.

我们将算法 UnmRadIdeDec 的步骤 U1 修改为：

U1. 用算法 IrrCharSer, IrrCharSerE 或 IrrTriSer 计算 $\mathbb{P}$ 的不可约特征序列 Φ, 且命 $\Phi\leftarrow\{\mathbb{T}\in\Phi:\ |\mathbb{T}|\le|\mathbb{P}|\}$, $\Psi\leftarrow\emptyset$.

此外，删除 UnmRadIdeDec 中的检测步骤 U3 (它在素理想的情形是不必要的). 现将所得的算法命名为 IrrVarDec, 并对其说明如下.

算法 IrrVarDec: $\Psi\leftarrow\mathrm{IrrVarDec}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P}\subset\mathcal{K}[\boldsymbol{x}]$, 本算法计算有限多个多项式组 $\mathbb{P}_1,\cdots,\mathbb{P}_e$ 构成的集合 Ψ, 使得分解 (6.2.9) 成立，该分解是极小的，并且每个 $\mathbb{P}_i$ 都定义一不可约代数簇.

例 6.2.1　设代数簇 $\mathcal{V}$ 由 $\mathbb{P}=\{P_1,P_2,P_3\}$ 所定义，其中

$$\begin{aligned}
P_1&=3\,x_3x_4-x_2^2+2\,x_1-2,\\
P_2&=3\,x_1^2x_4+4\,x_2x_3+6\,x_1x_3-2\,x_2^2-3\,x_1x_2,\\
P_3&=3\,x_3^2x_4+x_1x_4-x_2^2x_3-x_2.
\end{aligned}$$

关于变元序 $x_1 \prec \cdots \prec x_4$, $\mathbb{P}$ 可以分解为两个不可约三角列 $\mathbb{T}_1$ 和 $\mathbb{T}_2$, 使得

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{T}_1/2\,x_2 + 3\,x_1^2) \cup \mathrm{Zero}(\mathbb{T}_2/x_2),$$

这里

$$\begin{aligned}
\mathbb{T}_1 &= [T_1, T_2, 2\,x_2x_4 + 3\,x_1^2x_4 - 2\,x_2^2 - 3\,x_1x_2],\\
\mathbb{T}_2 &= [x_1, 2\,x_3 - x_2, 3\,x_2x_4 - 2\,x_2^2 - 4];\\
T_1 &= 2\,x_2^4 - 12\,x_1^2x_2^3 + 9\,x_1x_2^3 - 9\,x_1^4x_2^2 + 8\,x_1x_2^2 - 8\,x_2^2\\
&\quad + 24\,x_1^3x_2 - 24\,x_1^2x_2 + 18\,x_1^5 - 18\,x_1^4,\\
T_2 &= 2\,x_2x_3 + 3\,x_1^2x_3 - x_2^2.
\end{aligned}$$

为了求得 $\mathcal{V}$ 的不可约分解，我们按引理 6.2.3 分别计算

$$\mathbb{T}_1 \cup \left\{z\,(2\,x_2 + 3\,x_1^2) - 1\right\}, \quad \mathbb{T}_2 \cup \{x_2z - 1\}$$

的格罗布讷基 $\mathbb{G}_1, \mathbb{G}_2$ 以确定 $\mathbb{T}_1$ 和 $\mathbb{T}_2$ 的素基. 计算表明，$\mathbb{G}_1$ 和 $\mathbb{G}_2$ 分别由 8 个和 4 个多项式组成. 令 $\mathbb{V}_i = \mathbb{G}_i \cap \mathrm{Q}[x_1, \cdots, x_4]$, $\mathcal{V}_i = \mathrm{Zero}(\mathbb{V}_i)$, $i = 1, 2$. 我们有

$$\mathbb{V}_1 = \left[\begin{array}{l}
T_1,\\
27\,x_1^4x_3 - 27\,x_1^3x_3 + 2\,x_2^3 - 15\,x_1^2x_2^2 + 9\,x_1x_2^2 + 8\,x_1x_2\\
\qquad - 8\,x_2 + 12\,x_1^3 - 12\,x_1^2,\\
T_2,\\
12\,x_1x_3^2 - 12\,x_3^2 - 9\,x_1^2x_3 - 2\,x_1x_2^2 + 3\,x_2^2 + 4\,x_1^2 - 4\,x_1,\\
x_1x_4 - 2\,x_1x_3 + 2\,x_3 - x_2,\\
x_2x_4 + 3\,x_1^2x_3 - 3\,x_1x_3 - x_2^2,\\
P_1
\end{array}\right]$$

和 $\mathbb{V}_2 = \mathbb{T}_2$, 使得 $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$. 容易检验，这一分解是极小的.

例 6.2.2 考虑

$$\mathbb{P} = \left\{\begin{array}{l}
3\,x^2 - 4\,y^2 + z^2 + 4\,xz - 8\,yz - 4\,x + 1,\\
x^2 + 2\,y^2 + xz + 2\,yz - 2\,x - y - 3\,z
\end{array}\right\}$$

定义的代数曲线，它是三维空间中两个代数曲面的交. 关于变元序 $z \prec y \prec x$, 该曲线可以分解为两个不可约分支，其定义多项式组为

$$\mathbb{P}_1 = \{2y-1, x+z\},$$

$$\mathbb{P}_2 = \left\{\begin{array}{l} 50y^3+140zy^2-5y^2+94z^2y-58zy-24y-6z^3 \\ \qquad -74z^2-42z-5, \\ zx+2x-10y^2-14zy+3y+z^2+9z+1, \\ 5yx-13x+70y^2+99zy-29y-6z^2-75z-9, \\ x^2-4x+12y^2+16zy-4y-z^2-12z-1 \end{array}\right\};$$

第一个分支是一条直线，而第二个分支为一条三次挠线. 除了平面 $z+2=0$ 上的点外，$\mathbb{P}_2$ 中第三和第四个多项式可以去掉. 在平面 $z+2=0$ 上，三次挠线有一个实点和两个复点

$$\left(2, \frac{1}{2}, -2\right), \quad \left(2 \pm \frac{3}{5}\sqrt{-7}, \frac{13}{5}, -2\right).$$

图 4 对 $-5 \le x \le 5$ 绘制了这两条曲线的实部.

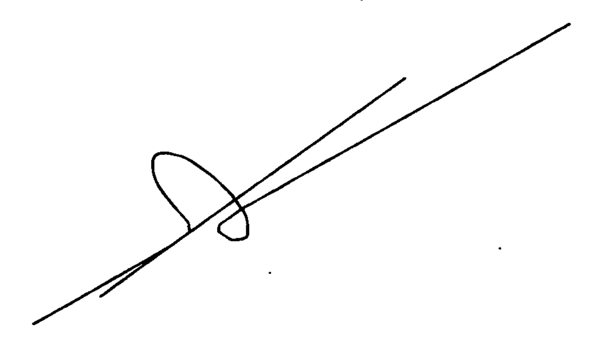


图 4 代数曲线

例 6.2.3 作为一个较复杂的例子，考虑下列 5 个多项式:

$$\begin{aligned}
P_1 &= a_{20}a_{11} + a_{21} + a_{11}a_{02} + 3a_{03}, \\
P_2 &= 54a_{20}a_{03} + 9a_{20}a_{11}a_{02} - 9a_{21}a_{02} - 9a_{11}a_{12} - 18a_{30}a_{11} - 2a_{11}^3, \\
P_3 &= 18a_{30}a_{03} - 9a_{20}^2a_{03} + 3a_{30}a_{11}a_{02} + 3a_{20}a_{02}a_{21} + 3a_{20}a_{12}a_{11} \\
&\quad - 3a_{21}a_{12} - 3a_{30}a_{21} - 2a_{11}^2a_{21}, \\
P_4 &= 3a_{30}a_{21}a_{02} + 3a_{30}a_{11}a_{12} + 3a_{20}a_{21}a_{12} - 18a_{20}a_{30}a_{03} - 2a_{11}a_{21}^2, \\
P_5 &= 9a_{30}a_{21}a_{12} - 27a_{30}^2a_{03} - 2a_{21}^3
\end{aligned}$$

所定义的代数簇. 命 $\mathbb{P}=\{P_1,\cdots,P_5\}$, 并设变元序为 ω_1: $a_{21}\prec a_{11}\prec a_{30}\prec a_{20}\prec a_{03}\prec a_{02}\prec a_{12}$. 在 ω_1 之下, $\mathbb{P}$ 可以分解为九个不可约三角列 $\mathbb{T}_i$, 使得

$$\mathrm{Zero}(\mathbb{P})=\bigcup_{i=1}^{9}\mathrm{Zero}(\mathbb{T}_i/\mathrm{ini}(\mathbb{T}_i)),$$

这里

$$\begin{aligned}
\mathbb{T}_1 &= [9\,a_{11}^2a_{30}^3+2\,a_{21}^2a_{11}^2a_{30}+2\,a_{21}^4, a_{21}a_{11}a_{20}-a_{11}^2a_{30}+a_{21}^2, P_1, P_2],\\
\mathbb{T}_2 &= [729\,a_{30}^6+81\,a_{11}^2a_{30}^5-243\,a_{21}^2a_{30}^4+36\,a_{21}^2a_{11}^2a_{30}^3+4\,a_{21}^4a_{11}^2a_{30}\\
&\quad + 4\,a_{21}^6, I_2a_{20}+2\,a_{21}a_{11}\,(81\,a_{30}^4+27\,a_{11}^2a_{30}^3-9\,a_{21}^2a_{30}^2\\
&\quad - 2\,a_{21}^2a_{11}^2a_{30}-6\,a_{21}^4)\,a_{30}, T_3, P_1, P_2],\\
\mathbb{T}_3 &= [a_{21}, a_{11}, a_{03}],\\
\mathbb{T}_4 &= [a_{21}, a_{30}, a_{20}, a_{11}a_{02}+3\,a_{03}, 9\,a_{12}+2\,a_{11}^2],\\
\mathbb{T}_5 &= [a_{21}, a_{30}, 9\,a_{20}^2+2\,a_{11}^2, a_{11}a_{02}+3\,a_{03}+a_{11}a_{20},\\
&\quad - 9\,a_{11}a_{12}+9\,a_{11}a_{20}a_{02}+54\,a_{20}a_{03}-2\,a_{11}^3],\\
\mathbb{T}_6 &= [a_{11}, 9\,a_{30}^2+a_{21}^2, a_{20}, 3\,a_{03}+a_{21}, a_{02}, a_{12}+3\,a_{30}],\\
\mathbb{T}_7 &= [a_{11}, 9\,a_{30}^2-2\,a_{21}^2, a_{20}^2+3\,a_{30}, 3\,a_{03}+a_{21}, a_{02}+2\,a_{20},\\
&\quad a_{12}+2\,a_{20}^2+6\,a_{30}],\\
\mathbb{T}_8 &= [32\,a_{11}^8+981\,a_{21}^2a_{11}^4-324\,a_{21}^4, T, 729\,a_{21}^3a_{20}-64\,a_{11}^7-2034\,a_{21}^2a_{11}^3,\\
&\quad T_3, P_1, P_2],\\
\mathbb{T}_9 &= [4\,a_{11}^8+36\,a_{21}^2a_{11}^4-81\,a_{21}^4, T, 1114656730\,a_{11}^5a_{20}\\
&\quad - 2077680789\,a_{21}^2a_{11}a_{20}+1576363572\,a_{21}a_{11}^4-2938274496\,a_{21}^3,\\
&\quad T_3, P_1, P_2];
\end{aligned}$$

$$\begin{aligned}
T &= -(128\,a_{11}^{12}-2430\,a_{21}^2a_{11}^8+6885\,a_{21}^4a_{11}^4-8748\,a_{21}^6)\,a_{11}^2a_{30}\\
&\quad + 3\,a_{21}^2\,(972\,a_{21}^6-675\,a_{11}^4a_{21}^4+570\,a_{11}^8a_{21}^2-80\,a_{11}^{12}),\\
T_3 &= I_3a_{03}+9\,a_{11}^3a_{20}^3+27\,a_{11}^3a_{30}a_{20}+2\,a_{11}^5a_{20}+4\,a_{21}a_{11}^4+9\,a_{21}^3;\\
I_2 &= 81\,a_{11}^2a_{30}^5-54\,a_{21}^2a_{11}^2a_{30}^3-18\,a_{21}^4a_{30}^2+4\,a_{21}^6,\\
I_3 &= 27\,(a_{21}a_{11}a_{20}-a_{11}^2a_{30}+a_{21}^2).
\end{aligned}$$

对 $i=6,\cdots,9$, 三角列 $\mathbb{T}_i$ 中多项式的个数都大于 5, 因此依引理 6.2.9, 对代数簇分解这些三角列都不必考虑. 设 $\mathbb{V}_i$ 为 $\mathbb{T}_i$ 在序 ω_1 之下的素基, $i=3,4,5$.

显然 $\mathbb{T}_3$ 本身已定义了一个不可约代数簇，于是 $\mathbb{V}_3 = \mathbb{T}_3$. 余下的是要按引理 6.2.3 确定 $\mathbb{T}_1, \mathbb{T}_2, \mathbb{T}_4$ 和 $\mathbb{T}_5$ 的素基. 不难发现，$\mathbb{V}_4 = \mathbb{T}_4$，而 $\mathbb{V}_5$ 与用

$$9\,a_{12} + 9\,a_{20}a_{02} - 2\,a_{11}^2$$

替换 $\mathbb{T}_5$ 中的最后一个多项式所得的多项式组相同. $\mathbb{T}_1$ 在 ω_1 之下的素基含有 20 个多项式. 为了减少元素的个数，我们将这一素基转换为另一变元序 ω_2: $a_{20} \prec a_{11} \prec a_{02} \prec a_{30} \prec a_{21} \prec a_{12} \prec a_{03}$ 之下的格罗布讷基. 新基 $\mathbb{V}_1$ 由 10 个多项式组成:

$$\mathbb{V}_1 = \begin{bmatrix} 81\,a_{30}^3 + 72\,a_{11}^2a_{30}^2 + 16\,a_{11}^4a_{30} + 90\,a_{20}^2a_{11}^2a_{30} + 4\,a_{20}^2a_{11}^4 \\ \quad +\ 18\,a_{20}^4a_{11}^2, \\ 6\,a_{20}a_{11}^2a_{21} + 9\,a_{20}^3a_{21} - 9\,a_{11}a_{30}^2 - 4\,a_{11}^3a_{30} + 9\,a_{20}^2a_{11}a_{30} \\ \quad +\ 2\,a_{20}^2a_{11}^3 + 9\,a_{20}^4a_{11}, \\ 9\,a_{30}a_{21} + 4\,a_{11}^2a_{21} + 9\,a_{20}^2a_{21} + 18\,a_{20}a_{11}a_{30} + 2\,a_{20}a_{11}^3 \\ \quad +\ 9\,a_{20}^3a_{11}, \\ a_{21}^2 + a_{20}a_{11}a_{21} - a_{11}^2a_{30}, \\ 9\,a_{20}^3a_{12} - 6\,a_{20}a_{11}a_{02}a_{21} - 12\,a_{20}^2a_{11}a_{21} + 9\,a_{02}a_{30}^2 \\ \quad +\ 18\,a_{20}a_{30}^2 + 4\,a_{11}^2a_{02}a_{30} - 9\,a_{20}^2a_{02}a_{30} + 8\,a_{20}a_{11}^2a_{30} \\ \quad -\ 2\,a_{20}^2a_{11}^2a_{02} - 2\,a_{20}^3a_{11}^2, \\ 9\,a_{11}a_{12} + 9\,a_{02}a_{21} + 18\,a_{20}a_{21} + 18\,a_{11}a_{30} + 9\,a_{20}a_{11}a_{02} \\ \quad +\ 2\,a_{11}^3 + 18\,a_{20}^2a_{11}, \\ 9\,a_{30}a_{12} + 9\,a_{20}^2a_{12} - 4\,a_{11}a_{02}a_{21} - 8\,a_{20}a_{11}a_{21} + 18\,a_{30}^2 \\ \quad -\ 9\,a_{20}a_{02}a_{30} + 2\,a_{11}^2a_{30} - 2\,a_{20}a_{11}^2a_{02} - 2\,a_{20}^2a_{11}^2, \\ 9\,a_{21}a_{12} - 6\,a_{11}^2a_{21} - 18\,a_{20}^2a_{21} + 9\,a_{11}a_{02}a_{30} \\ \quad -\ 18\,a_{20}a_{11}a_{30} - 4\,a_{20}a_{11}^3 - 18\,a_{20}^3a_{11}, \\ 81\,a_{12}^2 + 81\,a_{20}a_{02}a_{12} - 162\,a_{20}^2a_{12} + 108\,a_{11}a_{02}a_{21} \\ \quad +\ 216\,a_{20}a_{11}a_{21} - 324\,a_{30}^2 - 81\,a_{02}^2a_{30} + 162\,a_{20}a_{02}a_{30} \\ \quad -\ 72\,a_{11}^2a_{30} + 54\,a_{20}a_{11}^2a_{02} - 4\,a_{11}^4 + 36\,a_{20}^2a_{11}^2, \\ P_1 \end{bmatrix}.$$

对于 $\mathbb{T}_2$ 这一困难情形，用 T_i 表示 $\mathbb{T}_2$ 中的第 i 个多项式，而 I_i 表示 T_i 的初式，$1 \le i \le 5$. 非常数初式为

$$I_2,\quad I_3 \quad 和 \quad I_4 = I_5 = a_{11}.$$

因此，有必要通过计算扩大了的多项式组如 $\mathbb{T}_2 \cup \{z_1 I_4 - 1, z_2 I_3 - 1, z_3 I_2 - 1\}$ 或 $\mathbb{T}_2 \cup \{z I_2 I_3 I_4 - 1\}$ 的格罗布讷基来确定 $\mathbb{T}_2$ 的素基. 然而，无论在哪种情形格罗布讷基都不易计算. 我们尝试了一些最有效的格罗布讷基软件包而未能成功. 因此，我们用 Norm 将 $\mathbb{T}_2$ 正规化以求得另一三角列 $\mathbb{T}_2^*$: 该三角列是由 $\mathbb{T}_2$ 分别用

$$\begin{aligned}
T_2^* &= -4\, a_{21}^3 a_{11} a_{20} + 81\, a_{30}^4 + 9\, a_{11}^2 a_{30}^3 - 9\, a_{21}^2 a_{30}^2 + 6\, a_{21}^2 a_{11}^2 a_{30} - 2\, a_{21}^4, \\
T_3^* &= 972\, a_{21}^7 a_{03} + 729\,(2\, a_{11}^4 + 27\, a_{21}^2)\, a_{11}^2 a_{30}^5 \\
&\quad + 81\,(2\, a_{11}^8 + 9\, a_{21}^2 a_{11}^4 - 81\, a_{21}^4)\, a_{30}^4 - 648\, a_{21}^2\,(a_{11}^4 + 9\, a_{21}^2)\, a_{11}^2 a_{30}^3 \\
&\quad + 9\, a_{21}^2\,(8\, a_{11}^8 + 180\, a_{21}^2 a_{11}^4 + 81\, a_{21}^4)\, a_{30}^2 \\
&\quad - 36\, a_{21}^4\,(2\, a_{11}^4 + 27\, a_{21}^2)\, a_{11}^2 a_{30} + 2\, a_{21}^4\,(4\, a_{11}^8 + 90\, a_{21}^2 a_{11}^4 + 243\, a_{21}^4)
\end{aligned}$$

替换 T_2 和 T_3 所得. $\mathbb{T}_2^*$ 和 $\mathbb{T}_2$ 有相同的一般零点集，因而它们的素基定义相同的不可约代数簇. $\mathbb{T}_2^*$ 具有以下性质：其多项式的初式都只含参量 a_{21} 和 a_{11}.

按引理 6.2.3 计算相应的关于变元序 ω_1 或 ω_2 的格罗布讷基，我们容易求得 $\mathbb{T}_2^*$ 的素基. 该基在 ω_2 之下含有 9 个元素，陈列如下：

$$\mathbb{V}_2 = \left[\begin{array}{l}
81\, a_{20}^3 a_{02}^2 + 16\, a_{11}^4 a_{02} + 108\, a_{20}^2 a_{11}^2 a_{02} + 324\, a_{20}^4 a_{02} \\
\qquad + 20\, a_{20} a_{11}^4 + 144\, a_{20}^3 a_{11}^2 + 324\, a_{20}^5, \\
144\, a_{11}^2 a_{30} + 729\, a_{20}^2 a_{30} + 81\, a_{20}^3 a_{02} + 16\, a_{11}^4 + 144\, a_{20}^2 a_{11}^2 \\
\qquad + 405\, a_{20}^4, \\
4\, a_{02} a_{30} + 5\, a_{20} a_{30} + a_{20}^2 a_{02} + a_{20}^3, \\
4\, a_{11} a_{21} + 27\, a_{20} a_{30} + 2\, a_{20} a_{11}^2 + 9\, a_{20}^3, \\
18\, a_{02} a_{21} + 36\, a_{20} a_{21} - 18\, a_{11} a_{30} + 9\, a_{20} a_{11} a_{02} - 2\, a_{11}^3, \\
972\, a_{20} a_{30} a_{21} + 324\, a_{20}^3 a_{21} - 1296\, a_{11} a_{30}^2 - 405\, a_{20}^2 a_{11} a_{30} \\
\qquad + 81\, a_{20}^3 a_{11} a_{02} + 16\, a_{11}^5 + 108\, a_{20}^2 a_{11}^3 + 243\, a_{20}^4 a_{11}, \\
144\, a_{21}^2 + 1296\, a_{30}^2 - 81\, a_{20}^2 a_{30} - 81\, a_{20}^3 a_{02} - 16\, a_{11}^4 \\
\qquad - 144\, a_{20}^2 a_{11}^2 - 405\, a_{20}^4, \\
6\, a_{12} + 18\, a_{30} + 3\, a_{20} a_{02} + 2\, a_{11}^2 + 12\, a_{20}^2, \\
P_1
\end{array}\right].$$

容易验证，$\mathrm{Zero}(\mathbb{V}_4)$ 和 $\mathrm{Zero}(\mathbb{V}_5)$ 都是 $\mathrm{Zero}(\mathbb{V}_1)$ 的子代数簇. 因此 $\mathbb{P}$ 所定义的代数簇分解为三个由 $\mathbb{V}_1, \mathbb{V}_2$ 和 $\mathbb{V}_3$ 定义的不可约子代数簇. 用符号表示，即

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{V}_1) \cup \mathrm{Zero}(\mathbb{V}_2) \cup \mathrm{Zero}(\mathbb{V}_3), \tag{6.2.11}$$

其中 $\mathrm{Zero}(\mathbb{V}_i)$ 都不可约，$i = 1, 2, 3$.

上面的例子来自平面微分系统的定性研究. 我们将在 9.5 节中讨论其背景并使用所得的分解.

代数簇相除

我们说明如何将一个子代数簇从任一给定代数簇中除去. 这是用一个多项式除另一多项式的推广. 这种除法对多项式因子分解特别有用: 一个因子一旦发现就可以立即从被分解的多项式中除去. 可是, 除去子代数簇从计算上来讲要困难得多. 这种除法可按下述定理并入分解算法.

定理 6.2.18 设 $\mathbb{P}$ 和 $\mathbb{Q}=\{F_1,\cdots,F_t\}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式组, 且 $\mathrm{Zero}(\mathbb{Q})\subset\mathrm{Zero}(\mathbb{P})$. 又设 $\mathfrak{I}$ 为

$$\mathbb{P}\cup\{zF_1+\cdots+z^tF_t-1\}\ \text{在}\ \mathcal{K}[\boldsymbol{x},z]\ \text{中} \tag{6.2.12}$$

或者

$$\mathbb{P}\cup\{z_1F_1+\cdots+z_tF_t-1\}\ \text{在}\ \mathcal{K}[\boldsymbol{x},z_1,\cdots,z_t]\ \text{中} \tag{6.2.13}$$

生成的理想, 这里 $z,z_1,\cdots,z_t$ 均为新变元, 则

$$\mathrm{Zero}(\mathbb{P})=\mathrm{Zero}(\mathbb{Q})\cup\mathrm{Zero}(\mathfrak{I}\cap\mathcal{K}[\boldsymbol{x}]).$$

证 考虑

$$\mathfrak{I}=\mathrm{Ideal}(\mathbb{P}\cup\{zF_1+\cdots+z^tF_t-1\})$$

的情形. 设 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P})$. 对任意 $P\in\mathfrak{I}\cap\mathcal{K}[\boldsymbol{x}]$, 存在多项式 $Q\in\mathcal{K}[\boldsymbol{x},z]$, 使得

$$P-Q(zF_1+\cdots+z^tF_t-1)\in\mathrm{Ideal}(\mathbb{P})\subset\mathcal{K}[\boldsymbol{x},z].$$

所以对任意 z 有

$$P(\bar{\boldsymbol{x}})=Q(\bar{\boldsymbol{x}},z)[zF_1(\bar{\boldsymbol{x}})+\cdots+z^tF_t(\bar{\boldsymbol{x}})-1]. \tag{6.2.14}$$

假设 $\bar{\boldsymbol{x}}\notin\mathrm{Zero}(\mathbb{Q})$, 则存在 j, 使得 $F_j(\bar{\boldsymbol{x}})\neq 0$. 因此存在 $\bar{z}\in\tilde{\mathcal{K}}$, 使得

$$\bar{z}F_1(\bar{\boldsymbol{x}})+\cdots+\bar{z}^tF_t(\bar{\boldsymbol{x}})-1=0.$$

将 $\bar{z}$ 代入 (6.2.14) 即得 $P(\bar{\boldsymbol{x}})=0$. 所以 $\mathrm{Zero}(\mathbb{P})\subset\mathrm{Zero}(\mathbb{Q})\cup\mathrm{Zero}(\mathfrak{I}\cap\mathcal{K}[\boldsymbol{x}])$.

显然在 $\mathcal{K}[\boldsymbol{x},z]$ 中有 $\mathbb{P}\subset\mathfrak{I}$. 由于 $\mathbb{P}$ 中的所有多项式都不含 z, 故 $\mathbb{P}\subset\mathfrak{I}\cap\mathcal{K}[\boldsymbol{x}]$. 所以 $\mathrm{Zero}(\mathfrak{I}\cap\mathcal{K}[\boldsymbol{x}])\subset\mathrm{Zero}(\mathbb{P})$.

情形 $\mathfrak{I}=\mathrm{Ideal}(\mathbb{P}\cup\{z_1F_1+\cdots+z_tF_t-1\})$ 的证明类似, 只需注意如下事实: 如果 $F_1(\bar{\boldsymbol{x}}),\cdots,F_t(\bar{\boldsymbol{x}})$ 不全为 0, 则存在 $\bar{z}_1,\cdots,\bar{z}_t$, 使得 $\bar{z}_1F_1(\bar{\boldsymbol{x}})+\cdots+\bar{z}_tF_t(\bar{\boldsymbol{x}})-1=0$. □

上述定理提供了一种办法，它可以通过确定理想 $\mathfrak{I} \cap \mathcal{K}[\boldsymbol{x}]$ 的有限基 $\mathbb{H}$ 将任一子代数簇 Zero($\mathbb{Q}$) 从给定代数簇 Zero($\mathbb{P}$) 中除去. $\mathbb{H}$ 的确定可以通过计算 (6.2.12) 或 (6.2.13) 关于 $x_j \prec z$ 或 $x_j \prec z_l$ 决定的纯字典序格罗布纳基，以及其消元性质 (定理 5.3.5). 因此，分解 Zero($\mathbb{P}$) 化为分解 Zero($\mathbb{Q}$) 和 Zero($\mathbb{H}$). 我们用该技巧作了一些试验. 可是，此时格罗布纳基很难计算，我们从实验中未有所获. 看来这一技巧只有在确定有限基的程序比较有效时才会实用.

事实上，将 Zero($\mathbb{Q}$) 从 Zero($\mathbb{P}$) 中除去相当于计算商 Ideal($\mathbb{P}$) : Ideal($\mathbb{Q}$) (见定义 6.4.2). 后者可以用著作 [21] 中 (第 193 至 195 页) 描述的一个可能更有效的算法.

6.3 理想及根理想的从属关系

多项式理想论中的一个基本问题是从属关系的检验，即确定任一给定多项式是否属于一个给定生成元的理想 (见 [71] 第 58 页). 格罗布纳基最卓越的应用之一是给出了该问题的一个算法解. 具体来说，我们有如下定理.

定理 6.3.1 设 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$ 为多项式组，而 $\mathbb{G}$ 为 $\mathbb{P}$ 的格罗布纳基，则对任意多项式 $P \in \mathcal{K}[\boldsymbol{x}]$,

$$P \in \text{Ideal}(\mathbb{P}) \iff \text{rem}(P, \mathbb{G}) = 0.$$

该定理可以从 $\mathbb{P}$ 的格罗布纳基之定义和定理 5.3.2 (b) 得出.

推论 6.3.2 设 $\mathbb{P}, \mathbb{Q} \subset \mathcal{K}[\boldsymbol{x}]$ 为多项式组，而 $\mathbb{G}$ 为 $\mathbb{P}$ 的格罗布纳基，则

$$\text{Ideal}(\mathbb{Q}) \subset \text{Ideal}(\mathbb{P}) \iff \text{rem}(\mathbb{Q}, \mathbb{G}) = \{0\}.$$

例 6.3.1 考虑多项式

$$G_1 = x_1 x_4^2 + x_2 x_3 - 3\,x_1 x_2^2 + 3\,x_1 x_2 - x_1,$$
$$G_2 = 2\,x_2 x_4 + x_3 - 2\,x_1 x_2^2 - 2\,x_2 - 1$$

以及例 2.2.3 中的 $\mathbb{P}$. 多项式组 $\mathbb{P}$ 的格罗布纳基 $\mathbb{G}$ 已在例 5.3.1 中求得. 可以验证 $\text{rem}(G_1, \mathbb{G}) = 0$, 而 $\text{rem}(G_2, \mathbb{G}) \neq 0$. 所以

$$G_1 \in \text{Ideal}(\mathbb{P}), \quad G_2 \notin \text{Ideal}(\mathbb{P}),$$

且 $\text{Ideal}(\{G_1, G_2\}) \not\subset \text{Ideal}(\mathbb{P})$.

与检验多项式理想的从属关系形成对照，有诸多方法可以用来检验根理想的从属关系. 我们将本书中介绍的各种方法总结为如下定理. 现用 $\mathrm{SS}(\mathfrak{P})$ 和 $\mathrm{RS}(\mathfrak{P})$ 分别表示 $\mathcal{K}[\boldsymbol{x}]$ 中多项式组或系统 $\mathfrak{P}$ 的任意 *简单序列* 和 *正则序列*..

定理 6.3.3 设 P 为 $\mathcal{K}[\boldsymbol{x}]$ 中的任意多项式，$\mathbb{P}$ 为一多项式组，而 $\mathbb{P}^* = \mathbb{P} \cup \{zP-1\}$, 其中 z 为新变元，那么下列条件等价：

(a) $P \in \sqrt{\mathrm{Ideal}(\mathbb{P})}$;

(b) $\mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(P)$;

(c) $\mathrm{GB}(\mathbb{P}^*) = [1]$;

(d) $\mathrm{ITS}([\mathbb{P}, \{P\}]) = \mathrm{ITS}(\mathbb{P}^*) = \emptyset$;

(e) $\mathrm{SS}([\mathbb{P}, \{P\}]) = \mathrm{SS}(\mathbb{P}^*) = \emptyset$;

(f) $\mathrm{RS}([\mathbb{P}, \{P\}]) = \mathrm{RS}(\mathbb{P}^*) = \emptyset$;

(g) $\mathrm{TriSerP}(\mathbb{P}, \{P\}, 0) = \mathrm{TriSerP}(\mathbb{P}^*, \emptyset, 0) = \emptyset$;

(h) $\mathrm{prem}(P, \mathbb{T}) = 0$ 对所有 $\mathbb{T} \in \mathrm{ITS}(\mathbb{P})$ 成立;

(i) $\mathrm{prem}(P, \mathbb{T}) = 0$ 对所有 $[\mathbb{T}, \tilde{\mathbb{T}}] \in \mathrm{SS}(\mathbb{P})$ 成立.

证　首先注意：$\mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(P)$ 当且仅当 $\mathrm{Zero}(\mathbb{P}/P) = \emptyset$ 当且仅当 $\mathrm{Zero}(\mathbb{P}^*) = \emptyset$.

(a) $\Longleftrightarrow$ (b): 定理 1.6.3 和 $\sqrt{\mathrm{Ideal}(\mathbb{P})}$ 的定义.

(b) $\Longleftrightarrow$ (c): 推论 5.3.4.

(b) $\Longleftrightarrow$ (d): 推论 4.5.6.

(b) $\Longleftrightarrow$ (e): 定理 3.4.3 (a).

(b) $\Longleftrightarrow$ (f): 推论 3.2.17.

(b) $\Longleftrightarrow$ (g): 算法 TriSerP 中条件 (a) 和 (c).

(b) $\Longleftrightarrow$ (h): 定义 2.2.7 和推论 4.5.9.

(b) $\Longleftrightarrow$ (i): 定义 3.3.3 和定理 3.4.4. □

上述定理的直接推论是检验代数簇之间包含关系的各种方法.

例 6.3.2 回顾例 2.2.3 中的多项式组 $\mathbb{P}$ 和例 6.3.1 中的多项式 G_1 与 G_2. 由于 $\mathbb{P}\cup\{zG_1-1\}$ 关于序 $x_1\prec\cdots\prec x_4\prec z$ 的特征列是矛盾的, 所以 $G_1\in\sqrt{\mathrm{Ideal}(\mathbb{P})}$ (此时无需进一步分解). 若按定理 6.3.3 (d) 确定

$$G_2\notin\sqrt{\mathrm{Ideal}(\mathbb{P})},\tag{6.3.1}$$

则需要不可约分解.

用其他算法也能得到同样结论. 如果用定理 6.3.3 (h) 确定关系 (6.3.1), 我们同时得知从属关系对分支 $\mathbb{C}_1',\mathbb{C}_2''$ 和 $\mathbb{C}_4$ 不成立 (这些分支已在例 4.4.1 中给出).

例 6.3.3 设理想 $\mathfrak{I}$ 由下列多项式生成:

$$\begin{aligned}P_1&=def-abc,\\P_2&=4\,e^2f+3\,a^2c,\\P_3&=175\,bd^2ef+192\,ad^3f-108\,b^3ce.\end{aligned}$$

关于 $b\prec d\prec a\prec e\prec f\prec c$ 决定的全幂序,

$$\begin{aligned}\mathbb{G}=[&4\,b^3e^2c+3\,b^2daec,4\,baec+3\,da^2c,\\&-108\,b^3ec+175\,b^2dac+192\,d^3af,P_2,P_1]\end{aligned}$$

为 $\mathfrak{I}$ 的格罗布讷基. 令

$$G=8\,b^2ac-20\,bdef-9\,d^2af.$$

不难验证 $\mathrm{rem}(G,\mathbb{G})\neq 0$, 而 $\mathrm{rem}(G^2,\mathbb{G})=0$. 所以 $G\notin\mathfrak{I}$, 但 $G\in\sqrt{\mathfrak{I}}$. 按照定理 6.3.3, 也可用其他方法以不同方式获得结论 $G\in\sqrt{\mathfrak{I}}$.

根理想从属关系检验的一个重要应用是几何定理机器证明. 我们将在第八章中详细论述这一应用.

6.4 理想的准素分解

将多项式理想分解为准素分支是交换代数中的经典课题. 本节中, 我们说明如何从相应代数簇的不可约分解构造任意多项式理想的准素分解. 所使用的局部化和开方技巧是由下山武司和横山和弘 [66] 提出的.

定义 6.4.1 $\mathcal{K}[\boldsymbol{x}]$ 中两个理想 $\mathfrak{I}$ 和 $\mathfrak{J}$ 的 交, 记为 $\mathfrak{I}\cap\mathfrak{J}$, 是既属于 $\mathfrak{I}$ 又属于 $\mathfrak{J}$ 的所有多项式组成的集合.

定义 6.4.2 设 $\mathfrak{I}$ 和 $\mathfrak{J}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的理想. 称无限多个多项式组成的集合

$$\mathfrak{I}:\mathfrak{J} \triangleq \{F \in \mathcal{K}[\boldsymbol{x}]:\ FG \in \mathfrak{I} \text{ 对所有 } G \in \mathfrak{J} \text{ 成立}\}$$

为 $\mathfrak{I}$ 和 $\mathfrak{J}$ 的 *理想商*.

容易证明, $\mathcal{K}[\boldsymbol{x}]$ 中两个理想的交仍是理想, 而且它们的商也是如此 (见 [21] 第 185 和 193 页). $\mathfrak{I}:\mathfrak{J}$ 明显包含 $\mathfrak{I}$. 对任意多项式 F, 我们将 $\mathfrak{I}:\mathrm{Ideal}(\{F\})$ 简写为 $\mathfrak{I}:F$.

引理 6.4.1 设 $\mathfrak{I}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的理想, F 为多项式, 而 k 为正整数, 则

$$\mathfrak{I}:F^{\infty} = \mathfrak{I}:F^{k} \iff \mathfrak{I}:F^{k} = \mathfrak{I}:F^{k+1}.$$

作为推论, 可以通过计算 $\mathfrak{I}:F^{i}$ (其中 i 从 1 开始递增) 来确定最小的 k.

证 见课本 [21] 中 (196 页) 的练习. □

定义 6.4.3 理想 $\mathfrak{I} \subset \mathcal{K}[\boldsymbol{x}]$ 称为是 *伪准素的*, 如果 $\sqrt{\mathfrak{I}}$ 是素理想.
$\mathfrak{I}$ 称为是 *准素的*, 如果 $FG \in \mathfrak{I}$ 和 $F \notin \mathfrak{I}$ 蕴涵着存在正整数 q, 使得 $G^{q} \in \mathfrak{I}$.

定义 6.4.4 设 $\mathfrak{I}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的理想, 而 $\{\boldsymbol{u}\}$ 为 $\{\boldsymbol{x}\}$ 的子集. 称 $\{\boldsymbol{u}\}$ 为模 $\mathfrak{I}$ 的 *极大无关集*, 如果

$$\mathfrak{I} \cap \mathcal{K}[\boldsymbol{u}] = \{0\}, \quad \text{且} \quad \mathfrak{I} \cap \mathcal{K}[\boldsymbol{u}, x] \neq \{0\},\ \forall x \in \{\boldsymbol{x}\} \setminus \{\boldsymbol{u}\}.$$

引理 6.4.2 设 $\mathfrak{I}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的素理想, 而 $\mathbb{G}$ 为 $\mathfrak{I}$ 关于任一容许项序的格罗布讷基, 则 $\{\boldsymbol{u}\}$ 为模 $\mathfrak{I}$ 的极大无关集当且仅当

$$\mathrm{lt}(\mathbb{G}) \cap \mathrm{ter}(\boldsymbol{u}) = \emptyset, \quad \text{而} \quad \mathrm{lt}(\mathbb{G}) \cap \mathrm{ter}(\boldsymbol{u}, x) \neq \emptyset,\ \forall x \in \{\boldsymbol{x}\} \setminus \{\boldsymbol{u}\},$$

这里 $\mathrm{lt}(\mathbb{G}) \triangleq \{\mathrm{lt}(G):\ G \in \mathbb{G}\}$, $\mathrm{ter}(\boldsymbol{u})$ 表示所有关于 $\boldsymbol{u}$ 的项构成的集合, 而 $\mathrm{ter}(\boldsymbol{u}, x)$ 与之类似.

证 见文献 [66] 中定义 A.9 和引理 A.12. □

从不可约代数簇分解 (6.2.10) 或 (6.2.9) 立即可得 $\mathbb{P}$ 生成的根理想之分解如下:

$$\sqrt{\mathfrak{I}} = \bigcap_{i=1}^{e} \mathfrak{I}_i,$$

其中 $\mathfrak{I} = \text{Ideal}(\mathbb{P})$, $\mathfrak{I}_i = \text{Ideal}(\mathbb{P}_i)$, $1 \le i \le e$. 又由算法中的构造可知，每个 $\mathbb{P}_i$ 都是格罗布纳基，且 $\mathfrak{I}_i$ 是素的. 以下，我们构造伪准素理想 $\mathfrak{J}_i$, 使得 $\mathfrak{I}_i$ 是 $\mathfrak{J}_i$ 的相伴素理想，$1 \le i \le e$. 同时也将构造一个附加理想 $\mathfrak{I}^*$ 以得到如下分解：

$$\mathfrak{I} = \bigcap_{i=1}^{e} \mathfrak{J}_i \cap \mathfrak{I}^*. \tag{6.4.1}$$

若 $e = 1$, 则 $\mathfrak{I}$ 已是伪准素的. 现假定 $e > 1$, 对 $i \neq j$ 选取多项式 $S_{ij} \in \mathbb{P}_j \setminus \mathfrak{I}_i$, 并令

$$S_i = \prod_{\substack{1 \le j \le e \\ j \neq i}} S_{ij},$$

那么 $\mathfrak{J}_i = \mathfrak{I} : S_i^{\infty}$ 即是我们要求的伪准素理想. 欲求附加理想 $\mathfrak{I}^*$, 对每个 i 设 k_i 为使得 $\mathfrak{I} : S_i^{k_i} = \mathfrak{J}_i$ 的整数，则

$$\mathfrak{I}^* = \text{Ideal}(\mathbb{P} \cup \{S_1^{k_1}, \cdots, S_e^{k_e}\}).$$

从每个格罗布纳基 $\mathbb{G}$ 生成的伪准素理想 $\mathfrak{J}$, 可以用开方法确定一准素理想如次.

设 $\{\boldsymbol{u}\}$ 为模 $\sqrt{\mathfrak{J}}$ 的极大无关集，它可依引理 6.4.2 求得，而 $\{\boldsymbol{y}\} = \{\boldsymbol{x}\} \setminus \{\boldsymbol{u}\}$. 计算 $\mathbb{G}$ 关于 $u_j \prec y_l$ (对任意 $u_j \in \{\boldsymbol{u}\}, y_l \in \{\boldsymbol{y}\}$) 决定的纯字典序 ω 的格罗布纳基 $\bar{\mathbb{G}}$ 以及开方器

$$F = \text{lcm}(\{\text{lc}(G) \colon\ G \in \bar{\mathbb{G}}\}),$$

这里 $\text{lc}(G)$ 是 G 作为 $\mathcal{K}(\boldsymbol{u})[\boldsymbol{y}]$ 中的多项式关于序 ω 的导系数.

令 $\bar{\mathfrak{J}} = \text{Ideal}(\mathbb{G}) : F^{\infty}$. 按照引理 6.4.1, 可计算整数 k, 使得

$$\text{Ideal}(\mathbb{G}) : F^k = \bar{\mathfrak{J}}.$$

因此

$$\mathfrak{J} = \bar{\mathfrak{J}} \cap \text{Ideal}(\mathbb{G} \cup \{F^k\}),$$

且 $\bar{\mathfrak{J}}$ 为准素理想.

将以上过程用于理想 $\mathfrak{I}^*$ 和 $\text{Ideal}(\mathbb{G} \cup \{F^k\})$ 并递归进行，我们将进一步得到形如 (6.4.1) 的分解. 这一程序将会终止，最后给出理想分解

$$\mathfrak{I} = \bigcap_{i=1}^{h} \mathfrak{J}_i,$$

其中每个 $\mathfrak{J}_i$ 都是准素的.

现将上述分解程序写成算法如下.

算法 PriIdeDec: $\Psi \leftarrow \mathrm{PriIdeDec}(\mathbb{P})$. 任给非空多项式组 $\mathbb{P} \subset \mathcal{K}[\boldsymbol{x}]$, 本算法计算有限多个多项式组 $\mathbb{P}_1, \cdots, \mathbb{P}_h$ 构成的集合 Ψ, 使得

$$\mathrm{Ideal}(\mathbb{P}) = \bigcap_{i=1}^{h} \mathrm{Ideal}(\mathbb{P}_i),$$

且每个 $\mathrm{Ideal}(\mathbb{P}_i)$ 都是准素的.

P1. 命 $\Phi \leftarrow \{\mathbb{P}\}$, $\Psi \leftarrow \emptyset$.

P2. 重复下列步骤直至 $\Phi = \emptyset$:

P2.1. 设 $\mathbb{F}$ 为 Φ 中的元素, 且命 $\Phi \leftarrow \Phi \setminus \{\mathbb{F}\}$.

P2.2. 计算 $\Gamma \leftarrow \mathrm{IrrVarDec}(\mathbb{F})$. 若 $\Gamma = \emptyset$, 则转至 P2. 设 $\mathbb{F}_1, \cdots, \mathbb{F}_e$ 为 Γ 中的所有多项式组, 它们均为格罗布讷基.

P2.3. 对 $i = 1, \cdots, e$ 执行下列步骤:

P2.3.1. 命 $\mathbb{S} \leftarrow \emptyset$. 若 $e = 1$, 则命 $S \leftarrow 1, \mathbb{G} \leftarrow \mathbb{F}_1$ 并转至 P2.3.3. 否则, 对 $1 \leq j \leq e$ 和 $j \neq i$ 选取 $S_j \in \mathbb{F}_j \setminus \mathrm{Ideal}(\mathbb{F}_i)$, 且命

$$S \leftarrow \prod_{\substack{1 \leq j \leq e \\ j \neq i}} S_j.$$

P2.3.2. 按引理 6.2.3 计算 $\mathrm{Ideal}(\mathbb{F}) : S^\infty$ 的有限基, 并设该有限基为格罗布讷基 $\mathbb{G}$.

P2.3.3. 按引理 6.4.2 计算模 $\mathrm{Ideal}(\mathbb{F}_i)$ 的极大无关集 $\{\boldsymbol{u}\}$, 且令 $\{\boldsymbol{y}\} \leftarrow \{\boldsymbol{x}\} \setminus \{\boldsymbol{u}\}$.

P2.3.4. 计算 $\mathbb{G}$ 关于 $u_k \prec y_l$ (对任意 $u_k \in \{\boldsymbol{u}\}, y_l \in \{\boldsymbol{y}\}$) 决定的纯字典序 ω 的格罗布讷基 $\bar{\mathbb{G}}$ 以及关于序 ω 的开方器

$$F \leftarrow \mathrm{lcm}(\{\mathrm{lc}(G) \colon\ G \in \bar{\mathbb{G}} \subset \mathcal{K}(\boldsymbol{u})[\boldsymbol{y}]\}).$$

P2.3.5. 按引理 6.2.3 计算 $\mathrm{Ideal}(\mathbb{G}) : F^\infty$ 的有限基, 设其为格罗布讷基 $\mathbb{G}^*$, 且命 $\Psi \leftarrow \Psi \cup \{\mathbb{G}^*\}$.

P2.3.6. 按引理 6.4.1 计算整数 k 和 l, 使得

$$\mathrm{Ideal}(\mathbb{G}) : F^k = \mathrm{Ideal}(\mathbb{G}^*), \quad \mathrm{Ideal}(\mathbb{F}) : S^l = \mathrm{Ideal}(\mathbb{G}),$$

且命 $\Phi \leftarrow \Phi \cup \{\mathbb{G} \cup \{F^k\}\}, \mathbb{S} \leftarrow \mathbb{S} \cup \{S^l\}$.

P2.4. 命 $\Phi \leftarrow \Phi \cup \{\mathbb{F} \cup \mathbb{S}\}$.

关于 PriIdeDec 的证明以及改进该算法的各种技巧和策略，有兴趣的读者可以参阅 [66].

例 6.4.1 例 6.2.1, 6.2.2 和 6.3.1 中 $\mathbb{P}$ 生成的理想都是根理想. 它们中间每个都含有两个准素分支.

例 6.4.2 例 6.3.3 中给出的理想 $\mathfrak{I}$ (关于变元序 $b \prec d \prec a \prec e \prec f \prec c$) 可以分解为 8 个准素理想 $\mathfrak{I}_1, \cdots, \mathfrak{I}_8$. $\mathfrak{I}_i$ 的生成元及其相伴素理想如下表所示.

$\mathfrak{I}_i$	$\mathfrak{I}_i$ 的生成元	$\mathfrak{I}_i$ 的相伴素理想之生成元
$\mathfrak{I}_1$	$[a, e]$	$[a, e]$
$\mathfrak{I}_2$	$[f, c]$	$[f, c]$
$\mathfrak{I}_3$	$[a^2, F_1, ae, e^2, P_1, F_2^2]$	$[a, e, F_2]$
$\mathfrak{I}_4$	$\begin{bmatrix} a^2, 27\,be - 64\,da, ae, e^2, \\ 27\,b^2c - 64\,d^2f, P_1 \end{bmatrix}$	$[a, e, 27\,b^2c - 64\,d^2f]$
$\mathfrak{I}_5$	$[F_1, F_2, P_1, F_3]$	$[F_1, F_2, P_1, F_3]$
$\mathfrak{I}_6$	$[F_1^3, F_1 f, f^2, F_2, P_1, F_3, F_1 c, fc, c^2]$	$[F_1, f, c]$
$\mathfrak{I}_7$	$[d^2, F_1 e, de^2, e^3, dc, P_1, F_3, ec, c^2]$	$[d, e, c]$
$\mathfrak{I}_8$	$\begin{bmatrix} b^8, b^7a, b^6a^2, b^5a^3, b^4a^4, b^3a^5, b^2a^6, \\ ba^7, a^8, b^2F_1, aF_1, b^6f, b^5af, b^4a^2f, \\ b^3a^3f, b^2a^4f, ba^5f, a^6f, F_1f, b^4f^2, \\ b^3af^2, b^2a^2f^2, ba^3f^2, a^4f^2, b^2f^3, \\ baf^3, a^2f^3, f^4, bF_2, P_1, F_3, F_2f \end{bmatrix}$	$[b, a, f]$

表中

$$F_1 = 4\,be + 3\,da, \quad F_2 = 4\,b^2c + 3\,d^2f, \quad F_3 = 3\,a^2c + 4\,e^2f,$$

而 P_1 如例 6.3.3 所示.

注 6.4.1 我们最后指出，本书中研究的各种分解算法都有明显的并行特色，因而很容易并行化. 大部分算法都是计算分解树，对此不同的分支可以用并行处理器来分别处理. 并行计算方面的讨论已经超出了本书的范围，但几乎可以肯定这些算法经过适当并行化并在并行机上实施之后，其效力将会成倍增加. 笔者在 [77] 中报告了利用工作站网络将基于特征列的若干算法并行化的初步实验.

第七章 解代数方程组

消去法在众多科技、工程和工业领域中有形形色色的应用. 这些应用的详尽介绍可以占用一本书的篇幅. 本章和下两章中选择性地讨论若干这类应用问题, 其中多半与几何有关.

7.1 一 般 原 理

众所周知, 解代数方程是最基本的数学问题之一, 而诸多实际应用问题又都可以化为方程求解, 特别是多项式方程和不等方程组的求解. 前几章介绍的各种零点分解自然适用于这种 (非线性) 代数方程组的求解问题. 作为解多项式系统的基本原理, 我们列出几条定理, 它们都是已证结果的推论. 在下几节中, 我们将一般原理和方法用于一些非平凡的实例.

下面所考虑的多项式都是关于变元 $\boldsymbol{x} = (x_1, \cdots, x_n)$, 其系数在 $\mathcal{K} = \mathsf{Q}(\boldsymbol{u}) = \mathsf{Q}(u_1, \cdots, u_d)$ 中, 除非另有说明. 我们现在关心的是如下形式的联立多项式方程和不等方程组:

$$P_1 = 0, \cdots, P_s = 0,\ Q_1 \neq 0, \cdots, Q_t \neq 0. \tag{7.1.1}$$

令 $\mathbb{P} = \{P_1, \cdots, P_s\}$, $\mathbb{Q} = \{Q_1, \cdots, Q_t\}$, 而 $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$. 我们经常将 (7.1.1) 简写为

$$\mathbb{P} = 0,\quad \mathbb{Q} \neq 0. \tag{7.1.2}$$

系统 (7.1.1) 或 (7.1.2) 称为在数域 $\tilde{\mathcal{K}} \supset \mathcal{K}$ 中是 *可解的*, 如果它在 $\tilde{\mathcal{K}}$ 中有解.

引理 7.1.1 设 $[\mathbb{T}, \mathbb{U}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的三角系统, 且 $|\mathbb{T}| = n$, 则

$$\mathbb{T} = 0,\quad \mathbb{U} \neq 0 \tag{7.1.3}$$

在 $\mathcal{K}$ 的任意扩域中最多有有限多个解. 系统 (7.1.3) 在 $\mathcal{K}$ 中的所有解都能精确求出.

若特别有 $d = 0$, 则 (7.1.3) 在 (实数域) R 和 (复数域) C 中的所有解都能近似求出.

证 因 $|\mathbb{T}| = n$, 故可将 $\mathbb{T}$ 中的第 i 个多项式 T_i 写成如下形式:

$$T_i = T_i(x_1, \cdots, x_i),$$

此时 $\mathrm{lv}(T_i) = x_i$. 所以, $x_1 = \bar{x}_1$ 是 $T_1 = 0$ 关于 x_1 在 $\mathcal{K}$ 中的解当且仅当 $x_1 - \bar{x}_1$ 是 T_1 在 $\mathcal{K}$ 上的因子. 于是, $T_1 = 0$ 关于 x_1 在 $\mathcal{K}$ 中的所有解可以通过计算 T_1 在 $\mathcal{K}$ 上的所有线性因子而求出.

如果对 $T_1 = 0$ 的每个解 $x_1 = \bar{x}_1$ 都存在 $U \in \mathbb{U}$, 使得 $U(\bar{x}_1, x_2, \cdots, x_n) = 0$, 那么 (7.1.3) 在 $\mathcal{K}$ 中无解. 否则的话, 考虑 $T_1 = 0$ 在 $\mathcal{K}$ 中使得对任意 $U \in \mathbb{U}$ 都有 $U(\bar{x}_1, x_2, \cdots, x_n) \neq 0$ 的那些解 $x_1 = \bar{x}_1$. 多项式 $T_2(\bar{x}_1, x_2)$ 显然属于 $\mathcal{K}[x_2]$, 因此 $T_2(\bar{x}_1, x_2) = 0$ 关于 x_2 在 $\mathcal{K}$ 中的所有解可按同样方式通过计算 $T_2(\bar{x}_1, x_2)$ 在 $\mathcal{K}$ 上的所有线性因子而得出.

如果对 $T_1 = 0, T_2 = 0$ 和 $I_2 \neq 0$ 的每组解 $x_1 = \bar{x}_1, x_2 = \bar{x}_2$ 都存在 $U \in \mathbb{U}$, 使得 $U(\bar{x}_1, \bar{x}_2, x_3, \cdots, x_n) = 0$, 那么 (7.1.3) 在 $\mathcal{K}$ 中无解. 否则, 我们选取其中使得对任意 $U \in \mathbb{U}$ 都有 $U(\bar{x}_1, \bar{x}_2, x_3, \cdots, x_n) \neq 0$ 的那些解, 那么多项式 $T_2(\bar{x}_1, \bar{x}_2, x_3)$ 属于 $\mathcal{K}[x_3]$, 因而 $T_2(\bar{x}_1, \bar{x}_2, x_3) = 0$ 关于 x_3 在 $\mathcal{K}$ 中的所有解都能通过计算 $T_3(\bar{x}_1, \bar{x}_2, x_3)$ 在 $\mathcal{K}$ 上的所有线性因子而求得.

如此下去, 我们最终或者得出 (7.1.3) 在 $\mathcal{K}$ 中无解的结论, 或者求出 (7.1.3) 在 $\mathcal{K}$ 中的所有解.

在 $d = 0$ 时, $\mathcal{K}$ 成为有理数域 Q. 这时, 多项式 T_i 的系数都是有理数. 因此, 我们可以用数值方法求 $T_1 = 0$ 关于 x_1 在 R 或 C 中的近似解.

如果对 $T_1 = 0$ 的每个解 $x_1 = \bar{x}_1$ 都存在 $U \in \mathbb{U}$, 使得 $U(\bar{x}_1, x_2, \cdots, x_n) = 0$ 近似成立, 那么 (7.1.3) 在 R 或 C 中无近似解. 否则, 我们考虑 $T_1 = 0$ 使得对任意 $U \in \mathbb{U}$ 都近似地有 $U(\bar{x}_1, x_2, \cdots, x_n) \neq 0$ 的那些解 $x_1 = \bar{x}_1$, 并求 $T_2(\bar{x}_1, x_2) = 0$ 关于 x_2 在 R 或 C 中的近似解. 换言之, 我们将解多项式系统化为解一元多项式方程或不等方程. 后者在 R 或 C 中的近似解可以用已知的数值分析方法求得. □

引理 7.1.2 设 $[\mathbb{T}, \mathbb{U}]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的正则系统, 或简单系统, 或不可约三角系统, 或具有投影性质的三角系统, 那么系统 (7.1.3) 必定在 $\mathcal{K}$ 的某一扩域中有解. 如果解的个数在 $\mathcal{K}$ 的代数闭包中是有限的, 则 $|\mathbb{T}| = n$.

证 第一个断言由定理 3.4.1, 4.5.3 和 3.2.13 以及定义 4.1.2 可得.

若 $|\mathbb{T}| < n$, 则可以从 $\mathcal{K}$ 中为 $\mathbb{T}$ 的参量选取无穷多组数值, 使得在参量被任意一组数值替换之后 $[\mathbb{T}, \mathbb{U}]$ 仍是完美的 (见例如定理 4.5.3 和 3.2.13 的证明). 所以, 此时 (7.1.3) 在 $\mathcal{K}$ 的代数闭包中有无穷多组解. □

对任意三角列 $\mathbb{T}$, $[\mathbb{T}, \mathrm{ini}(\mathbb{T})]$ 是 (特殊的) 三角系统. 因此, 上面的两个引理导出三角列的相应结果. 此外, 若 $\mathbb{T} = [T_1, \cdots, T_n]$ 而且对每个 i, $\mathbb{T}^{\{i\}} = 0$ 的任意解都不使 T_{i+1} 关于 x_{i+1} 的所有系数为零, 则 $\mathbb{T} = 0$ 在 $\mathcal{K}$ 的任一扩域中也最多只有有限多个解.

定理 7.1.3 设 Ψ 为 $\mathcal{K}[\boldsymbol{x}]$ 中任一多项式系统 $[\mathbb{P}, \mathbb{Q}]$ 的正则序列, 或简单序列, 或不可约三角序列, 或者是由算法 TriSerP 对 $k=0$ 计算所得的 $[\mathbb{P}, \mathbb{Q}]$ 的三角序列, 那么

(a) (7.1.2) 在 $\mathcal{K}$ 的任意扩域中都无解当且仅当 $\Psi = \emptyset$;

(b) (7.1.2) 最多有有限多组解当且仅当对每个 $[\mathbb{T}, \mathbb{U}] \in \Psi$ 都有 $|\mathbb{T}| = n$. 此时, (7.1.2) 的解可以通过对所有 $[\mathbb{T}, \mathbb{U}] \in \Psi$ 计算 $\mathbb{T} = 0, \mathbb{U} \neq 0$ 的解而求得.

证 (a) 见定理 3.4.3 (a), 推论 4.5.6 和 3.2.16, 以及 TriSerP 中的 (a) 和 (c).

(b) 见引理 7.1.1 和 7.1.2; 也请参阅定理 3.4.3 (b). □

解任意多项式方程和不等方程组 —— 通过将其化为三角系统 —— 的过程推广了中国矩阵法 (见 [5] 第 218 和 219 页) 和解线性方程组的高斯消去法. 格罗布讷基不一定是三角列, 但格罗布讷基的消元性质 (定理 5.3.5) 确保了变元的分离. 因而可以从相应的 (字典序) 格罗布讷基求得一组多项式方程的解, 此时可能需要一些附加的最大公因子计算. 有关细节, 参见下面给出的文献.

定理 7.1.4 设 $\mathbb{P}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式组, 而 $\mathbb{G} = \mathrm{GB}(\mathbb{P})$, 则

(a) $\mathbb{P} = 0$ 在 $\mathcal{K}$ 的任意扩域中都无解当且仅当 $\mathbb{G} = [1]$;

(b) $\mathbb{P} = 0$ 最多有有限多组解当且仅当对所有 i $(1 \leq i \leq n)$ 都存在整数 m_i 和多项式 $G_i \in \mathbb{G}$, 使得 $\mathrm{lt}(G_i) = x_i^{m_i}$;

(c) 如果 $\mathbb{P} = 0$ 只有有限多组解而 $\mathbb{G}$ 是用纯字典项序计算的, 那么所有在 $\mathcal{K}$ 中的解都能从 $\mathbb{G}$ 精确求出. 若又有 $d = 0$, 则所有在 R 和 C 中的解都能从 $\mathbb{G}$ 近似地求得.

证 (a) 见推论 5.3.4.

(b) 见 [8] 中方法 6.9.

(c) 见 [8] 中方法 6.10 和引理 7.1.1. □

定理 7.1.5 设 Ψ 为 $\mathbf{Q}[\boldsymbol{u},\boldsymbol{x}]$ 中多项式系统 $\mathfrak{P}$ 的正则序列或简单序列, 或者是由算法 TriSerP 对 $x_n,\cdots,x_1$ 投影 (即 $k=d$) 计算所得的 $\mathfrak{P}$ 的三角序列, 并假定 $\Psi\neq\emptyset$, 则

(a) 对任意 $[\mathbb{T},\mathbb{U}]\in\Psi$ 和 $\bar{\boldsymbol{u}}\in\tilde{\mathbf{Q}}^d$ (这里 $\tilde{\mathbf{Q}}\supset\mathbf{Q}$), 系统

$$(\mathbb{T}\setminus\mathbf{Q}[\boldsymbol{u}])|_{\boldsymbol{u}=\bar{\boldsymbol{u}}}=0,\quad (\mathbb{U}\setminus\mathbf{Q}[\boldsymbol{u}])|_{\boldsymbol{u}=\bar{\boldsymbol{u}}}\neq 0$$

关于 $\boldsymbol{x}$ 在 $\mathbf{C}$ 中有解当且仅当 $\boldsymbol{u}=\bar{\boldsymbol{u}}$ 是

$$\mathbb{T}\cap\mathbf{Q}[\boldsymbol{u}]=0,\quad \mathbb{U}\cap\mathbf{Q}[\boldsymbol{u}]\neq 0$$

的解;

(b)

$$\mathrm{Proj}_{\boldsymbol{u}}\mathrm{Zero}(\mathfrak{P})=\bigcup_{\mathfrak{T}\in\Psi}\mathrm{Proj}_{\boldsymbol{u}}\mathrm{Zero}(\mathfrak{T})=\bigcup_{[\mathbb{T},\mathbb{U}]\in\Psi}\mathrm{Zero}(\mathbb{T}\cap\mathbf{Q}[\boldsymbol{u}]/\mathbb{U}\cap\mathbf{Q}[\boldsymbol{u}]).$$

证 (a) 该充要条件由 (b) 可得.

(b) 见推论 3.2.14, 推论 3.4.2, 定义 3.3.3 和算法 TriSerP 中的条件 (b) 与 (c). □

7.2 解零维系统

按照前节的结果, 我们可以通过计算其正则序列、简单序列、不可约三角序列或格罗布讷基来确定任一给定多项式系统是否零维. 如果该系统是零维的因此只有有限多组解, 那么所有解都能从这些序列或格罗布讷基精确或近似地求出. 以下我们举若干实例以具体说明如何解零维系统.

例 7.2.1 首先考虑一个较简单的多项式方程组

$$\begin{cases} x_1x_2-1=0,\\ x_3^2+bx_1x_2=0,\\ bx_1x_3+x_2^2-x_1=0,\\ bx_2x_3-x_2+x_1^2=0. \end{cases}\tag{7.2.1}$$

设 $\mathbb{P}$ 为 (7.2.1) 式左边四个多项式组成的集合, 并将变元排序为 $b\prec x_1\prec x_2\prec x_3$. 从 $\mathbb{P}$,

- CharSer 计算的特征序列由下列两个升列组成:

$$\mathbb{C}_1=[b^3+4,x_1^3+1,x_1x_2-1,2\,x_3+b^2],\quad \mathbb{C}_2=[b,x_1^3-1,x_1x_2-1,x_3];$$

- TriSerS 计算的三角序列由两个三角系统 $[\mathbb{C}_1, \{b, x_1\}]$ 和 $[\mathbb{C}_2, \{x\}]$ 组成；若用 TriSer 计算，则所得三角序列由 $[\mathbb{T}_1, \{b, x_1\}]$ 和 $[\mathbb{T}_2, \{x\}]$ 组成，其中

$$\mathbb{T}_1 = [b^3+4, x_1^3+1, x_1x_2-1, bx_3-2],$$
$$\mathbb{T}_2 = [b, x_1^3-1, x_2-x_1^2, x_3],$$

  这里 $\mathbb{T}_1$ 和 $\mathbb{C}_1$ 中只有第四个元素不同，而 $\mathbb{T}_2$ 和 $\mathbb{C}_2$ 中只有第三个元素不同；

- RegSer 计算的正则序列和 SimSer 计算的简单序列相同，均由 $[\mathbb{T}_1, \emptyset]$ 和 $[\mathbb{C}_2, \emptyset]$ 组成；

- $\mathbb{P}$ 的格罗布讷基为

$$\mathbb{G} = [b^5+4\,b^2, 2\,x_1^3-b^3-2, 2\,x_2-b^3x_1^2-2\,x_1^2, 2\,bx_3+b^3, x_3^2+b].$$

无论在哪种情形,我们都能从三角化的多项式组依次求得 (7.2.1) 关于 b, x_1, x_2, x_3 的所有 12 组解. 这些解 (b, x_1, x_2, x_3) 如下所示:

$$(0,1,1,0), \qquad (0,-\alpha,-\beta,0), \qquad (0,-\beta,-\alpha,0),$$
$$\left(-\gamma,-1,-1,-\frac{\gamma^2}{2}\right), \quad \left(-\gamma,\alpha,\beta,-\frac{\gamma^2}{2}\right), \quad \left(-\gamma,\beta,\alpha,-\frac{\gamma^2}{2}\right),$$
$$\left(\alpha\gamma,-1,-1,\frac{\beta\gamma^2}{2}\right), \quad \left(\alpha\gamma,\alpha,\beta,\frac{\beta\gamma^2}{2}\right), \quad \left(\alpha\gamma,\beta,\alpha,\frac{\beta\gamma^2}{2}\right),$$
$$\left(\beta\gamma,-1,-1,\frac{\alpha\gamma^2}{2}\right), \quad \left(\beta\gamma,\alpha,\beta,\frac{\alpha\gamma^2}{2}\right), \quad \left(\beta\gamma,\beta,\alpha,\frac{\alpha\gamma^2}{2}\right),$$

其中

$$\alpha = \frac{1-\sqrt{-3}}{2}, \quad \beta = \frac{1+\sqrt{-3}}{2}, \quad \gamma = \sqrt[3]{4}.$$

下例所考虑的一组三个多项式方程的求解问题是德国莱比锡大学计算机科学系的黑默克等人公布的挑战. 他们在处理双摆的倾斜效应时遇到了该系统. 为了便于数值计算, 他们希望求得只含 p 的极小多项式 F, 使得所考虑的系统仅在 $\bar{p}$ 是 F 的实根时才有实解 $(\bar{p}, \bar{x}, \bar{y})$.

例 7.2.2 命 $\mathbb{P}=\{P_1,P_2,P_3\}$, 其中

$$
\begin{aligned}
P_1 = {} & F_1y^8-4xy^7+F_2y^6-4xy^5+2[(19p+7)x^2+19p-7]y^4\\
& +4xy^3+F_2y^2+4xy+F_1,\\
P_2 = {} & -F_3y^{10}+2(px^4+8x^2-p)y^9-F_4y^8+8(3px^4+4x^2-3p)y^7\\
& -F_5y^6+76p(x^4-1)y^5+F_5y^4+8(3px^4-4x^2-3p)y^3\\
& +F_4y^2+2(px^4-8x^2-p)y+F_3,\\
P_3 = {} & -[G_1-2(p-4)x^6-48x^4+2(p+4)x^2]y^{18}-H_1y^{17}\\
& -[G_2-2(99p-20)x^6+272x^4+2(99p+20)x^2]y^{16}-H_2y^{15}\\
& -[G_3-16(135p+12)x^6+2688x^4+48(45p-4)x^2]y^{14}-H_3y^{13}\\
& -[G_4-32(237p+40)x^6+8192x^4+32(237p-40)x^2]y^{12}-H_4y^{11}\\
& -[G_5-4(1969p+668)x^6+13472x^4+4(1969p-668)x^2]y^{10}-H_5y^9\\
& +[G_5+4(151p+668)x^6-13472x^4-4(151p-668)x^2]y^8-H_4y^7\\
& +[G_4-160(11p-8)x^6-8192x^4+160(11p+8)x^2]y^6-H_3y^5\\
& +[G_3-16(11p-12)x^6-2688x^4+16(11p+12)x^2]y^4-H_2y^3\\
& +[G_2-2(43p+20)x^6-272x^4+2(43p-20)x^2]y^2-H_1y\\
& +G_1-2(9p+4)x^6+48x^4+2(9p-4)x^2,
\end{aligned}
$$

而

$$
\begin{aligned}
& F_1=(p+1)x^2+p-1,\quad F_2=4[(3p+2)x^2+3p-2],\\
& F_3=2px(x^2+1),\quad F_4=22px(x^2+1),\quad F_5=52px(x^2+1),\\
& G_1=(p+1)px^8-2p^2x^4+(p-1)p,\\
& H_1=4p[(p-3)x^6+(p-5)x^4-(p+5)x^2-p-3]x,\\
& G_2=(23p+19)px^8-46p^2x^4+(23p-19)p,\\
& H_2=16p[(6p-7)x^6+(6p-5)x^4-(6p+5)x^2-6p-7]x,\\
& G_3=4(49p+32)px^8-392p^2x^4+4(49p-32)p,\\
& H_3=16p[(55p+1)x^6+11(5p-3)x^4-11(5p+3)x^2-55p+1]x,\\
& G_4=4(179p+86)px^8-1432p^2x^4+4(179p-86)p,\\
& H_4=16p[9(26p+15)x^6+(234p-379)x^4-(234p+379)x^2\\
& \qquad -9(26p-15)]x,\\
& G_5=6(133p+39)px^8-1596p^2x^4+6(133p-39)p,\\
& H_5=8p[(867p+511)x^6+(867p-1399)x^4-(867p+1399)x^2\\
& \qquad -867p+511]x.
\end{aligned}
$$

多项式 P_1, P_2 和 P_3 分别有 24, 26 和 172 项. 我们希望确定一个 p 的无平方因子的多项式 F, 使得 F 的每个不可约因子至少有一个实根, 并且对 F 的每个实根 $\bar{p}$, $\mathbb{P}|_{p=\bar{p}}$ 关于 x 和 y 都有实零点. 而且也希望给出相应的三角列, 由此那些实零点可以近似求出.

关于变元序 $y \prec x \prec p$, 用 IrrTriSer 计算的 $\mathbb{P}$ 的不可约三角序列由六个不可约三角列构成, 其中三个三角列含有多项式 y^2+1, 一个含有 y^4+6y^2+1; 因此这四个三角列显然没有实零点. 剩下的两个三角列之一很简单: $[y, x, p-1]$. 因而对 $p=1$ 多项式组 $\mathbb{P}$ 关于 (x, y) 有零点 $(0, 0)$. 另外一个三角列 $\mathbb{T}$ 由多项式

$$
\begin{aligned}
T_1 = {} & 5y^{26} + 119y^{24} - 1026y^{22} - 33198y^{20} - 73569y^{18} \\
& + 330381y^{16} - 826956y^{14} + 801228y^{12} - 541965y^{10} \\
& + 98593y^8 - 14738y^6 - 1086y^4 + 73y^2 - 5, \\
T_2 = {} & 2800229949440x^2 \\
& - (554715797135y^{24} + 13245948695838y^{22} \\
& - 112783397552632y^{20} - 3691969096634086y^{18} \\
& - 8453054312182633y^{16} + 35984613145186252y^{14} \\
& - 88904017316023032y^{12} + 81944347139116756y^{10} \\
& - 53872365946917715y^8 + 7072365366548726y^6 \\
& - 1416438227076176y^4 - 34613922094542y^2 \\
& - 27445391662739)yx - 2800229949440,
\end{aligned}
$$

和 $T_3 = P_1$ 组成. 为了从 $\mathbb{T}$ 得到一个仅含 p 的多项式, 我们计算 $\mathbb{T}$ 关于变元序 $p \prec y \prec x$ 的修正特征列 $\mathbb{C}$; $\mathbb{C}$ 是不可约的, 并由下列三个大整系数多项式组成:

$$
\begin{aligned}
C_1 = {} & 891956372701184p^{26} + 2068185729954043084 8p^{24} \\
& - 70356081438769503909p^{22} + 27168225069955575615 1p^{20} \\
& - 352622918902513898391p^{18} + 269322942095440399641p^{16} \\
& - 161495209483939229280p^{14} + 68524380500279748288p^{12} \\
& - 19025554366923988992p^{10} + 3272908595517318656p^8 \\
& - 337374627314737152p^6 + 22759224799248384p^4 \\
& - 932001922220032p^2 + 25389989167104, \\
C_2 = {} & C_{22}y^2 + C_{20}, \\
C_3 = {} & C_{31}yx - 127pC_{30},
\end{aligned}
$$

其中

$$
\begin{aligned}
C_{22} = {} & 97596069285814673617066118316032\,p^{24} \\
& + 2263021199504486735034281169688730256\,p^{22} \\
& - 6445128413689655108167040863584775863\,p^{20} \\
& + 262124222127959978004215590111392754659\,p^{18} \\
& - 24188175706696847911672006783733784096\,p^{16} \\
& + 16615541447884461140451486478479619488\,p^{14} \\
& - 8670364071094253213057783138290887552\,p^{12} \\
& + 2844615722290334148560991584871727104\,p^{10} \\
& - 535852172105963925589608448535918592\,p^{8} \\
& + 57733782999568794064532852443996160\,p^{6} \\
& - 4006630547637705936521457045307392\,p^{4} \\
& + 166718638115384143626225139384320\,p^{2} \\
& - 4653369315611714838187251073024,
\end{aligned}
$$

$$
\begin{aligned}
C_{20} = {} & 5190332949513881277892021747712\,p^{24} \\
& + 120352816228986627112501468145817456\,p^{22} \\
& - 312280408157439555186048343596998793\,p^{20} \\
& + 1317721164143429048825672081647752397\,p^{18} \\
& - 961242947684448643010631887677341816\,p^{16} \\
& + 674404246899577504198017002592901344\,p^{14} \\
& - 327559558971080229743822480554897536\,p^{12} \\
& + 94819899239384626079409119905130496\,p^{10} \\
& - 16628288137479442591930684997449728\,p^{8} \\
& + 1726044837932534863836342246121472\,p^{6} \\
& - 117151089195602183499827194920960\,p^{4} \\
& + 4806199355471889403131827257344\,p^{2} \\
& - 131821769666765033493404581888,
\end{aligned}
$$

$$
\begin{aligned}
C_{31} = {} & 37180685754903476153120456704\,p^{25} \\
& + 24706314470648654886471303168\,p^{24} \\
& + 862124500562923861565527409183232\,p^{23} \\
& + 572876529608495972342085018633648\,p^{22}
\end{aligned}
$$

$$
\begin{aligned}
& - 2625859311677581377286792763494332\,p^{21} \\
& - 1730408184448766074577801102200038\,p^{20} \\
& + 1043503826977866404291209896338725 4\,p^{19} \\
& + 6896470694766188219200982578632831\,p^{18} \\
& - 11093066044325708367270080030892672\,p^{17} \\
& - 7214490734073783049965212394082929\,p^{16} \\
& + 7747608910891368241052159204122656\,p^{15} \\
& + 5037485491901043179104189690450800\,p^{14} \\
& - 4243165118882995892452318320458880\,p^{13} \\
& - 2757459581652024395694746068269312\,p^{12} \\
& + 1517129008176375659586012812502528\,p^{11} \\
& + 989332732038604692490901481473280\,p^{10} \\
& - 304696265967449832058967795165184\,p^{9} \\
& - 199762630410549896488774599141888\,p^{8} \\
& + 33881392401694597659493187411968\,p^{7} \\
& + 22271692235350864758592015650816\,p^{6} \\
& - 2410501311591366398832035856384\,p^{5} \\
& - 1588600788508295375916088000512\,p^{4} \\
& + 101466217158638789838225801216\,p^{3} \\
& + 66933864467214475735656824832\,p^{2} \\
& - 2909343961680813477533843456\,p \\
& - 1925267368125917549668663296,
\end{aligned}
$$

$$
\begin{aligned}
C_{30} = & \ 547731310218996635386511 36\,p^{24} \\
& + 1270045527117656047383591766272\,p^{22} \\
& - 3927302324324801265181215734139\,p^{20} \\
& + 15484046099200925967336906647011\,p^{18} \\
& - 16867149760322976518797526099412\,p^{16} \\
& + 11404354396199128317753925881432\,p^{14} \\
& - 6134178436693360267186668138720\,p^{12} \\
& + 2155054429737018937187335296384\,p^{10} \\
& - 424467937326630860512467795456\,p^{8} \\
& + 46757697001909599373780649984\,p^{6}
\end{aligned}
$$

$$
\begin{aligned}
&- 32969658513014914753646837776\,p^4\\
&+ 138312759565055121045946368\,p^2\\
&- 3922536354990693960515584.
\end{aligned}
$$

因为 $\mathbb{T}$ 和 $\mathbb{C}$ 都是不可约的,且维数为 0, 而 $\mathrm{Zero}(\mathbb{C}) \subset \mathrm{Zero}(\mathbb{T})$, 所以 $\mathrm{Zero}(\mathbb{C}) = \mathrm{Zero}(\mathbb{T})$. 这里, 先使用序 $y \prec x \prec p$ 的想法归功于杨路, 他用不同的方法求得了这一挑战系统的解.

多项式 C_1 有四个实根 $-\gamma^*, -\gamma, \gamma, \gamma^*$, 其分离如下:

$$
-\gamma^* \in \left[-1, -\frac{3}{4}\right], \quad -\gamma \in [-\alpha, -\beta], \quad \gamma \in [\beta, \alpha], \quad \gamma^* \in \left[\frac{3}{4}, 1\right],
$$

这里

$$
\begin{aligned}
\alpha &= \frac{4968916493678842742821555}{4\,\mu},\\
\beta &= \frac{9937832987357685485643109}{8\,\mu};\\
\mu &= 2417851639229258349412352.
\end{aligned}
$$

令 $D(p) = -4\,C_{22}C_{20}$, 即 C_2 关于 y 的判别式; 它是一个 25 项的多项式, 关于 p 的次数为 48. 显然 $C_2|_{p=\bar{p}}$ 有实零点当且仅当 $D(\bar{p}) \geq 0$. D 也有四个实根

$$
-r_1 \in [-a, -b], \quad -r_2 \in [-c, -d], \quad r_2 \in [d, c], \quad r_1 \in [b, a],
$$

其中

$$
\begin{aligned}
a &= \frac{4968916493678842742821559}{4\,\mu},\\
b &= \frac{9937832987357685485643117}{8\,\mu},\\
c &= \frac{9937832987357685485641801}{8\,\mu},\\
d &= \frac{1242229123419710685705225}{\mu}.
\end{aligned}
$$

此时两个负根非常接近, 而两个正根亦是如此. 注意 $c < b$. 容易验证

$$
a < \frac{3}{4}, \quad \text{而} \quad D\left(\mp\frac{3}{4}\right) < 0,
$$

因此在 $p = \mp\gamma^*$ 时 C_2 关于 y 没有实零点.

因 $c<\beta$ 而 $\alpha<b$, 故

$$-\gamma\in(-r_1,-r_2),\quad \gamma\in(r_2,r_1).$$

又有 $D(\mp\alpha)>0$, 所以 $D(\mp\gamma)>0$. 另一方面, $\mathbb{C}$ 的不可约性保证了 $C_{22}(\mp\gamma)\neq 0$. 因而在 $p=\mp\gamma$ 时 C_2 关于 y 各有两个实零点. 实际上, 它关于 y 的所有四个实零点可以从上面的 T_1 分离得出.

由于 C_3 关于 x 是线性的, 它关于 x 的实零点之存在性显而易见. 综合上述, $\mathbb{C}$ 关于 (p,y,x) 有四组实零点:

$$(-\gamma,-\bar{y},\bar{x}_1),\quad(-\gamma,\bar{y},-\bar{x}_1),\quad(\gamma,-\bar{y},-\bar{x}_2),\quad(\gamma,\bar{y},\bar{x}_2).$$

$\gamma,\bar{y}$ 和 $\bar{x}_i$ 到 55 位的近似值如下:

$$\gamma=0.5137739236207634508235369242764404138533394611706909720,$$
$$\bar{y}=4.0391116900221207463389736986402650000203279157084119 49,$$
$$\bar{x}_1=1.3666774595158994264748894445900104561770043043599827 19,$$
$$\bar{x}_2=0.7317015386748363688691362102473370621081618037430149163.$$

于是, 欲求的极小多项式为 $F=(p-1)\,C_1$. 原来的多项式组 $\mathbb{P}$ 有五组实零点, 其中 p 取 F 五个实根中的三个.

下例说明如何在 $\mathbb{Q}$ 的任意函数域上解零维多项式系统.

例 7.2.3 考虑下列 8 个多项式方程组成的系统:

$$\begin{aligned}
P_1 &= u_3g_{00}+u_3h_{00}+u_3^2+u_2^2-u_1^2=0,\\
P_2 &= h_{11}+g_{11}=0,\\
P_3 &= h_{10}+g_{10}=0,\\
P_4 &= h_{01}+g_{01}=0,\\
P_5 &= u_3g_{00}h_{10}+u_3g_{10}h_{00}+u_1^2u_3g_{01}h_{11}+u_1^2u_3g_{11}h_{01}-2\,u_1^4g_{11}h_{11}\\
&\quad -2\,u_1^2g_{10}h_{10}-2\,u_1u_2g_{10}h_{10}-2\,u_1^3u_2g_{11}h_{11}=0,\\
P_6 &= 2\,u_1u_2u_3g_{01}h_{11}-2\,u_1^2u_3g_{11}h_{01}-2\,u_1^2u_3g_{01}h_{11}+2\,u_1u_2u_3g_{11}h_{01}\\
&\quad +u_3^2g_{01}h_{10}+u_3^2g_{00}h_{11}+u_3^2g_{11}h_{00}+u_3^2g_{10}h_{01}-2\,u_1^2u_3g_{11}h_{10}\\
&\quad -2\,u_1^2u_3g_{10}h_{11}-2\,u_1u_2u_3g_{10}h_{11}-4\,u_1^2u_2^2g_{11}h_{11}\\
&\quad -2\,u_1u_2u_3g_{11}h_{10}+4\,u_1^4g_{11}h_{11}=0,\\
P_7 &= u_1^2g_{01}h_{01}+u_1^2g_{10}h_{10}+u_1^4g_{11}h_{11}+g_{00}h_{00}+u_1^2=0,\\
P_8 &= u_3g_{01}h_{00}+2\,u_1u_2g_{01}h_{01}-2\,u_1^2g_{01}h_{01}+u_3g_{00}h_{01}\\
&\quad +2\,u_1^3u_2g_{11}h_{11}+u_1^2u_3g_{10}h_{11}-2\,u_1^4g_{11}h_{11}+u_1^2u_3g_{11}h_{10}=0.
\end{aligned}\tag{7.2.2}$$

我们希望求出 (7.2.2) 关于 h_{ij} 和 g_{ij} 在 $\mathrm{Q}(u_1,u_2,u_3)$ 中的一组解. 为此, 计算 $\{P_1,\cdots,P_8\}$ 关于变元序

$$h_{01} \prec h_{11} \prec h_{10} \prec h_{00} \prec g_{01} \prec g_{00} \prec g_{11} \prec g_{10}$$

的修正弱特征列 $\mathbb{C}$:

$$\mathbb{C} = \begin{bmatrix} 4\,u_1^2h_{01}^2 - u_2^2 - 2\,u_1u_2 - u_1^2, \\ u_1\,(u_2+u_1)\,h_{11} - u_3h_{01}, \\ (u_2+u_1)\,h_{10} + (u_2-u_1)\,h_{01}, \\ 2\,u_3h_{01}h_{00} + 2\,u_1^2u_3h_{11}h_{10} + 2\,u_1^3\,(u_2-u_1)\,h_{11}^2 \\ \quad + 2\,u_1\,(u_2-u_1)\,h_{01}^2 + (u_3^2+u_2^2-u_1^2)\,h_{01}, \\ g_{01} + h_{01}, \\ u_3g_{00} + u_3h_{00} + u_3^2 + u_2^2 - u_1^2, \\ g_{11} + h_{11}, \\ g_{10} + h_{10} \end{bmatrix},$$

它是拟线性的. $\mathbb{C}$ 中的第一个多项式在 Q 上的因子分解为

$$(2\,u_1h_{01} - u_2 - u_1)\,(2\,u_1h_{01} + u_2 + u_1).$$

不在 $\mathrm{Q}(u_1,u_2,u_3)$ 中的初式仅有 h_{01}. 因此容易通过解一元线性方程从以上三角列求得两组解. 我们列出其中之一供以后使用:

$$\begin{aligned} g_{11} &= \frac{u_3}{2\,u_1^2}, & h_{11} &= -\frac{u_3}{2\,u_1^2}, \\ g_{01} &= \frac{u_1+u_2}{2\,u_1}, & h_{01} &= -\frac{u_1+u_2}{2\,u_1}, \\ g_{10} &= \frac{u_1-u_2}{2\,u_1}, & h_{10} &= -\frac{u_1-u_2}{2\,u_1}, \\ g_{00} &= \frac{2\,u_1^2 - 2\,u_2^2 - u_3^2}{2\,u_3}, & h_{00} &= -\frac{u_3}{2}. \end{aligned} \tag{7.2.3}$$

通过计算 $\mathbb{P}$ 的三角、特征或格罗布讷序列, 可以发现 (7.2.2) 关于 h_{ij} 和 g_{ij} 在 $\mathrm{Q}(u_1,u_2,u_3)$ 中不再有其他解.

7.3 解高维系统

下例中的多项式系统源自罗仑兹所考虑的一个浑沌吸因子的动力系统. 文献 [52, 25] 中对此有过研究.

例 7.3.1 考虑多项式方程组

$$\begin{cases} P_1 = x_2\,(x_3 - x_4) - x_1 + c = 0, \\ P_2 = x_3\,(x_4 - x_1) - x_2 + c = 0, \\ P_3 = x_4\,(x_1 - x_2) - x_3 + c = 0, \\ P_4 = x_1\,(x_2 - x_3) - x_4 + c = 0. \end{cases}$$

令 $\mathbb{P} = \{P_1, \cdots, P_4\}$, 且 $c \prec x_1 \prec \cdots \prec x_4$. 用 IrrTriSer 可将 $\mathbb{P}$ 分解为 13 个不可约三角列. 若同时用 NormG 进行正规化, 则 IrrTriSer 可求得 11 个正规不可约三角列 $\mathbb{T}_i$, 使得

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{T}_1/F_1F_2) \cup \bigcup_{i=2}^{11} \mathrm{Zero}(\mathbb{T}_i),$$

其中

$$\mathbb{T}_1 = \left[\begin{array}{l} 2\,x_1^8 - 2\,(c-4)\,x_1^7 - 4\,(c-4)\,x_1^6 - 4\,(c+3)\,(c-2)\,x_1^5 \\ \quad -\ (3\,c^2 + 3\,c - 26)\,x_1^4 - (c^3 + c^2 - 20)\,x_1^3 + (c^2 + c + 12)\,x_1^2 \\ \quad +\ (c^3 + 3\,c^2 + 4)\,x_1 + 2\,c^2 + c + 1, \\ F_1F_2x_2 + 2\,(c^4 + 8\,c^3 - 8\,c^2 - 8\,c - 1)\,x_1^7 \\ \quad -\ 2\,(c^5 + 5\,c^4 - 23\,c^3 + 31\,c^2 + 30\,c + 4)\,x_1^6 \\ \quad -\ 2\,(c^5 - 6\,c^4 - 27\,c^3 + 67\,c^2 + 54\,c + 7)\,x_1^5 \\ \quad -\ 2\,(2\,c^6 + 17\,c^5 - 35\,c^4 - 34\,c^3 + 104\,c^2 + 73\,c + 9)\,x_1^4 \\ \quad +\ (c^6 + 39\,c^5 + 78\,c^4 + 2\,c^3 - 239\,c^2 - 137\,c - 16)\,x_1^3 \\ \quad -\ (c^7 + 10\,c^6 - 12\,c^5 - 16\,c^4 + 73\,c^3 + 190\,c^2 + 82\,c + 8)\,x_1^2 \\ \quad +\ (c^7 + 14\,c^6 - 2\,c^5 - 17\,c^4 - 45\,c^3 - 90\,c^2 - 34\,c - 3)\,x_1 \\ \quad +\ 3\,c^5 - 37\,c^4 - 28\,c^3 - 20\,c^2 + c + 1, \\ F_1F_2x_3 + 2\,(c^4 + 3\,c^3 + c^2 + 9\,c + 2)\,x_1^7 \\ \quad -\ 2\,(c^5 - 2\,c^4 - 13\,c^3 - 3\,c^2 - 32\,c - 7)\,x_1^6 \\ \quad -\ 2\,(3\,c^5 - 5\,c^4 - 21\,c^3 - 19\,c^2 - 58\,c - 12)\,x_1^5 \\ \quad -\ 2\,(2\,c^6 + 11\,c^5 - 14\,c^4 - 14\,c^3 - 40\,c^2 - 81\,c - 16)\,x_1^4 \\ \quad -\ (7\,c^6 + 30\,c^5 - 36\,c^4 - 68\,c^3 - 125\,c^2 - 162\,c - 30)\,x_1^3 \\ \quad -\ (c^7 + 11\,c^6 + 23\,c^5 - 62\,c^4 - 79\,c^3 - 123\,c^2 - 105\,c - 18)\,x_1^2 \\ \quad -\ (c^7 + 7\,c^6 - 10\,c^5 - 73\,c^4 - 65\,c^3 - 69\,c^2 - 54\,c - 9)\,x_1 \\ \quad +\ (c+1)\,(19\,c^4 + 33\,c^3 + 15\,c^2 + 11\,c + 2), \\ P_4 \end{array}\right],$$

$$\mathbb{T}_2 = [2\,x_1^2 - 2\,x_1 - c + 1, x_2 + x_1 - 1, x_3 - x_1, x_4 + x_1 - 1],$$
$$\mathbb{T}_3 = [x_1 - c, x_2 - c, x_3 - c, x_4 - c],$$
$$\mathbb{T}_4 = [F_1, x_1 + 2, x_2 + 2\,c + 1, x_3 + 2\,c + 1, x_4 - c],$$
$$\mathbb{T}_5 = [F_1, x_1 - c, x_2 + 2, x_3 + 2\,c + 1, x_4 + 2\,c + 1],$$
$$\mathbb{T}_6 = [F_1, x_1 + 2\,c + 1, x_2 - c, x_3 + 2, x_4 + 2\,c + 1],$$
$$\mathbb{T}_7 = [F_1, x_1 + 2\,c + 1, x_2 + 2\,c + 1, x_3 - c, x_4 + 2],$$

$$\mathbb{T}_8 = \begin{bmatrix} F_2, \\ 8\,x_1 + F, \\ 4\,x_2^2 - (c^3 + 12\,c^2 - 3\,c - 2)\,x_2 + c^3 + 12\,c^2 - c + 4, \\ 8\,x_3 - 2\,(c^3 + 12\,c^2 - 3\,c + 2)\,x_2 - (c-1)\,(c^2 + 12\,c + 3), \\ P_4 \end{bmatrix},$$

$$\mathbb{T}_9 = \begin{bmatrix} F_2, \\ 4\,x_1^2 - 2\,(c-1)\,x_1 - c^3 - 12\,c^2 + 3\,c + 2, \\ 8\,x_2 + F, \\ 2\,x_3 + (c^3 + 12\,c^2 - 2\,c + 5)\,x_1 + 2, \\ P_4 \end{bmatrix},$$

$$\mathbb{T}_{10} = \begin{bmatrix} F_2, \\ 4\,x_1^2 + (c^2 + 8\,c + 3)\,x_1 + c^3 + 13\,c^2 + 3\,c + 3, \\ 8\,x_2 + (3\,c^3 + 37\,c^2 + 5\,c + 3)\,x_1 + 2\,(c^2 + 12\,c - 5)\,c, \\ 8\,x_3 + F, \\ P_4 \end{bmatrix},$$

$$\mathbb{T}_{11} = \begin{bmatrix} F_2, \\ 4\,x_1^2 - (c^3 + 12\,c^2 - 3\,c - 2)\,x_1 + c^3 + 12\,c^2 - c + 4, \\ 8\,x_2 - 2\,(c^3 + 12\,c^2 - 3\,c + 2)\,x_1 - (c-1)\,(c^2 + 12\,c + 3), \\ 8\,x_3 - (c+1)\,(c^2 + 12\,c - 1)\,(x_1 + 1), \\ P_4 \end{bmatrix};$$

$$F_1 = 2\,c^2 + 2\,c + 1,$$
$$F_2 = c^4 + 12\,c^3 - 2\,c^2 + 4\,c + 1,$$
$$F = c^3 + 11\,c^2 - 13\,c + 9.$$

由这些三角列可知，所给多项式系统是一维的，因此关于 $c, x_1, \cdots, x_4$ 有无穷多组解. 对 c 的任意给定数值，该系统只有有限多组解. 所有这些解都能从 $\mathbb{T}_i$

求得.

与上述结果比较，我们发现文献 [25] 中给出的有些 p 链是多余的. 设 $\mathbb{G}_1$ 为 $\mathbb{T}_1$ 的素基，则由引理 6.2.9 得

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{G}_1) \cup \mathrm{Zero}(\mathbb{T}_2) \cup \mathrm{Zero}(\mathbb{T}_3).$$

对任意多项式 $P \in \mathcal{K}[\boldsymbol{x}]$, 我们用指标三元组 $[t\ \mathrm{lv}(P)\ \mathrm{ldeg}(P)]$ 来刻画 P, 其中 t 为 P 的项数.

下例中的多项式组 $\mathbb{P}$ 见于文献 [81], 它是由费交流给萨波尔和格德斯的.

例 7.3.2　考虑 $\mathbb{P} = \{P_1, \cdots, P_4\}$, 其中

$$\begin{aligned}
P_1 = {} & 2\,(b-1)^2 + 2\,(q - pq + p^2) + c^2\,(q-1)^2 - 2\,bq \\
& + 2\,cd\,(1-q)\,(q-p) + 2\,bpqd\,(d-c) + b^2d^2\,(1-2\,p) \\
& + 2\,bd^2\,(p-q) + 2\,bdc\,(p-1) + 2\,bpq\,(c+1) \\
& + (b^2 - 2\,b)\,p^2d^2 + 2\,b^2p^2 + 4\,b\,(1-b)\,p + d^2\,(p-q)^2, \\
P_2 = {} & d\,(2\,p+1)\,(q-p) + c\,(p+2)\,(1-q) + b\,(b-2)\,d \\
& + b\,(1-2\,b)\,pd + bc\,(q+p-pq-1) + b\,(b+1)\,p^2d, \\
P_3 = {} & -b^2\,(p-1)^2 + 2\,p\,(p-q) - 2\,(q-1), \\
P_4 = {} & b^2 + 4\,(p-q^2) + 3\,c^2\,(q-1)^2 - 3\,d^2\,(p-q)^2 \\
& + 3\,b^2d^2\,(p-1)^2 + b^2p\,(p-2) + 6\,bdc\,(p+q+pq-1).
\end{aligned}$$

视 b 为参量，并将其他变元排序为 $p \prec d \prec c \prec q$. 用 IrrTriSer 容易计算 $\mathbb{P}$ 的不可约三角序列，它由两个不可约三角列构成. 其中之一非常简单:

$$[p-1, d, bc+2, q-1];$$

另一三角列由四个多项式组成，其中前三个多项式的指标三元组为

$$[625\ p\ 23],\quad [373\ d\ 1],\quad [17\ c\ 1],$$

而最后一个多项式为 P_3.

至于计算 $\mathbb{P}$ 在 $\mathbb{Q}$ 上的三角序列 (即 b 不视为参量), 我们对几种变元序尝试了不同的算法都未能成功. 所出现的多项式非常大，因而计算无法在合理的时间内完成.

7.4 解参数系统

考虑形如 (7.1.1) 的多项式方程和不等方程组，其系数在 Q 中，而 $\boldsymbol{u}=(u_1,\cdots,u_d)$ 为 *参数*. 我们希望定出那些参数值，对此所考虑的系统关于未知数 x_i 在 Q 的某一扩域上有解，并求出那些解. 特别指出，这与例 7.2.3 中的情形不同；那里 u_1,u_2,u_3 被当做超越元，因而不取任何特定数值.

定理 7.1.5 指出如何解参数多项式系统：通过计算正则系统、简单系统或者任意具有投影性质的三角系统，我们可以确定对参数 $\boldsymbol{u}$ 的哪些值，系统 $\mathbb{P}=0,\mathbb{Q}\neq 0$ 关于未知数 $\boldsymbol{x}$ 有解 (参阅 [25]). 对任给参数值 $\bar{\boldsymbol{u}}$, 该系统的解可以从正则、简单或三角系统

$$[(\mathbb{T}\setminus \mathrm{Q}[\boldsymbol{u}])|_{\boldsymbol{u}=\bar{\boldsymbol{u}}},\ (\mathbb{U}\setminus \mathrm{Q}[\boldsymbol{u}])|_{\boldsymbol{u}=\bar{\boldsymbol{u}}}],\quad [\mathbb{T},\mathbb{U}]\in\Psi,$$

求出或者用其表示，这里 Ψ 与定理 7.1.5 中相同.

注 7.4.1 置 $\mathfrak{P}=[\mathbb{P},\mathbb{Q}]$. 算法 TriSerP 中的投影有些复杂，主要是为了保持零点分解

$$\mathrm{Zero}(\mathfrak{P})=\bigcup_{i=1}^{e}\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)$$

同时成立. 如果我们只需定出参数值 $\bar{\boldsymbol{u}}\in\tilde{\mathrm{Q}}^d$, 使得从 $\mathfrak{P}$ 通过用 $\bar{\boldsymbol{u}}$ 替换 $\boldsymbol{u}$ 所得的多项式系统关于变元 x_k 有零点，则可以对 TriSerP 进行简化；而那些关于 x_k 的零点可用三角系统 $[\mathbb{T}_i^{[0]},\mathbb{U}_i^{[0]}]$ 来表示或者由其求出.

容易看出，$\mathfrak{P}$ 的任一零点必定是某个 $[\mathbb{T}_i,\mathbb{U}_i]$ 的零点，而 $[\mathbb{T}_i,\mathbb{U}_i]$ 的每个零点是否也是 $\mathfrak{P}$ 的零点可以直接验证. 可是，为了保证 $[\mathbb{T}_i,\mathbb{U}_i]$ 的每个零点也一定是 $\mathfrak{P}$ 的零点 (而不必加以验证), 我们不得不像 ProjA 中那样收集 $\mathbb{U}^{[k]}$ 中的多项式，最后再将它们添入相应的 $\mathbb{U}_i$ (通过计算最大公因子有可能从 $\mathbb{U}_i$ 中去掉一些多项式).

例如，命 $P=x^2-u^2$, $D=x-u$, 其中 u 为参数，则

$$\begin{aligned}\mathrm{Proj}_u\mathrm{Zero}(P/D)&=\mathrm{Proj}_u\mathrm{Zero}(\emptyset/\mathrm{prem}(D^2,P))\\&=\mathrm{Proj}_u\mathrm{Zero}(\emptyset/uD)=\mathrm{Zero}(\emptyset/u).\end{aligned}$$

此时，零点 $(1,1)$ 属于 $\mathrm{Zero}(P/u)$ 但不属于 $\mathrm{Zero}(P/D)$, 所以 $\mathrm{Zero}(P/u)\neq\mathrm{Zero}(P/D)$. 这就表明，不能在投影过程中将多项式 D 抛弃. 保留 D, 我们有

$$\mathrm{Zero}(P/[u,D])=\mathrm{Zero}(P/D),$$

因此对任意 $\bar{u} \in \mathrm{Zero}(\emptyset/u)$, 系统

$$x^2 - \bar{u}^2 = 0,\ x - \bar{u} \neq 0$$

关于 x 有解，其解可从上面 (三角化) 的系统求得.

一种通过计算特征列 (与 TriSerP 类似) 的投影方法由吴文俊等人提出 (见 [103, 25]), 而文献 [25] 中未能对上面解释的问题作出正确处理.

例 7.4.1　参阅 [8, 25]. 对未知数 $x_1 \prec \cdots \prec x_4$ 求解

$$\begin{cases} P_1 = x_4 - a_4 + a_2 = 0, \\ P_2 = x_4 + x_3 + x_2 + x_1 - a_4 - a_3 - a_1 = 0, \\ P_3 = x_3x_4 + x_1x_4 + x_2x_3 + x_1x_3 - a_3a_4 - a_1a_4 - a_1a_3 = 0, \\ P_4 = x_1x_3x_4 - a_1a_3a_4 = 0, \end{cases}$$

其中 $a_1 \prec \cdots \prec a_4$ 为参数.

使用 IrrTriSer 和 NormG, 我们可以计算 $\mathbb{P} = \{P_1, \cdots, P_4\}$ 的不可约正规三角序列，该序列由下列九个不可约正规三角列组成:

$$\begin{aligned} \mathbb{T}_1 &= [Ix_1 - a_1a_3, Ix_2 + (I - a_1)(I - a_3), x_3 - a_4, x_4 - I], \\ \mathbb{T}_2 &= [Ix_1 - a_1a_4, Ix_2 - a_2(I - a_1), x_3 - a_3, x_4 - I], \\ \mathbb{T}_3 &= [Ix_1 - a_3a_4, Ix_2 - a_2(I - a_3), x_3 - a_1, x_4 - I], \\ \mathbb{T}_4 &= [a_1, I, x_2 + x_1 - a_2, x_3 - a_3, x_4], \\ \mathbb{T}_5 &= [a_1, I, x_2 + x_1 - a_3, x_3 - a_2, x_4], \\ \mathbb{T}_6 &= [a_2, a_4, x_2 + x_1 - a_1, x_3 - a_3, x_4], \\ \mathbb{T}_8 &= [a_2, a_4, x_2 + x_1 - a_3, x_3 - a_1, x_4], \\ \mathbb{T}_8 &= [a_3, I, x_2 + x_1 - a_1, x_3 - a_2, x_4], \\ \mathbb{T}_9 &= [a_3, I, x_2 + x_1 - a_2, x_3 - a_1, x_4], \end{aligned}$$

其中 $I = a_4 - a_2$, 使得

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{3} \mathrm{Zero}(\mathbb{T}_i/I) \cup \bigcup_{i=4}^{9} \mathrm{Zero}(\mathbb{T}_i).$$

从上面的 $\mathbb{T}_i$, 容易定出对 $a_1, \cdots, a_4$ 的哪些数值原来的方程组 $\mathbb{P} = 0$ 关于 $x_1, \cdots, x_4$ 有解. 对任意给定的参数值，那些解可以从相应的三角列精确求出 (三角列中的每个多项式关于其导元都是线性的).

也可以用 TriSerP 计算三角序列，或者用 RegSer 计算正则序列，或者用 SimSer 计算简单序列来解上述参数方程组．投影所得的三角序列与上面的不可约三角序列类似，而简单序列则含有更多的三角列，因此相对复杂．这里我们不再将它们列出．

例 7.4.2 参见例 3.3.5 中的多项式组 $\mathbb{P}$ 及其分解 (为简单系统)．不难验证

$$\bigcup_{j=1}^{13}\mathrm{Zero}(\mathbb{T}_j^{(1)}/\tilde{\mathbb{T}}_j^{(1)}) = \bigcup_{j=1}^{5}\mathrm{Zero}(\emptyset/\tilde{\mathbb{T}}_j)\cup\mathrm{Zero}(H_1)\cup\mathrm{Zero}(H_2)$$
$$\cup\,\mathrm{Zero}(c)\cup\mathrm{Zero}(2\,c^3-27)=\tilde{\mathbb{Q}}.$$

所以，多项式方程组 $\mathbb{P}=0$ 对 c (视为参数) 的任意数值都有解．在 c 的具体数值给定时，关于 z,y,x 的解可从相应的简单系统求得．

从前面给出的具有投影性质或正规化的三角系统和简单系统，可以求解下列参数系统：

$$\begin{cases}(x-u)^2+(y-v)^2-1=0,\\ v^2-u^3=0,\\ 2\,v\,(x-u)+3\,u^2\,(y-v)=0,\\ (3\,wu^2-1)\,(2\,wv-1)=0,\end{cases}$$

其中 $x\prec y$ 为参数，$u\prec v\prec w$ 为未知数 (见例 4.2.2)；

$$\begin{cases}x^2+y^2+z^2-r^2=0,\\ xy+z^2-1=0,\\ xyz-x^2-y^2-z+1=0,\end{cases}$$

其中 r 为参数，$z\prec y\prec x$ 为未知数 (见例 4.1.1 和 3.3.4)；

$$\begin{cases}z\,(x^2+y^2-c)+1=0,\\ y\,(x^2+z^2-c)+1=0,\\ x\,(y^2+z^2-c)+1=0,\end{cases}$$

其中 c 为未知数，$z\prec y\prec x$ 为未知数 (见例 3.3.5)；

$$\begin{cases}x_2\,(x_3-x_4)-x_1+c=0,\\ x_3\,(x_4-x_1)-x_2+c=0,\\ x_4\,(x_1-x_2)-x_3+c=0,\\ x_1\,(x_2-x_3)-x_4+c=0,\end{cases}$$

其中 c 为参数，$x_1\prec\cdots\prec x_4$ 为未知数 (见例 7.3.1)．

第八章 几何定理机器证明与发现

自吴文俊的开创性工作[94]以来，几何定理机器证明的研究十分活跃. 这一新兴学科中的文献非常丰富. 我们向希望深入了解该学科以及吴文俊方法精髓的读者推荐吴的原著[96]. 周咸青的论著[14]对吴方法亦有简明的介绍，并收集了大量证例. 关于该学科在 1996 年以前的状况，读者也可以参阅笔者的综述[87]和其中所列文献.

8.1 基本方法

关于几何定理机器证明，吴文俊及其追随者提出了各种成功有效的方法，其中大部分运用代数计算. 这些方法可以视为前面各章中介绍的种种消元技术的一个主要应用. 使用代数方法证明几何定理的第一步是将所考虑的几何问题代数化. 为此，我们选取一个坐标系，并用未定元 $x_1,\cdots,x_n$ 表示点的坐标以及其他几何量如三角形的面积、距离的平方等. 如此一来，大多数几何定理的假设和结论都可以用 $x_1,\cdots,x_n$ 的多项式方程 $(=)$, 不等方程 $(\neq)$ 和不等式 $(\leq,<)$ 来表达. 我们举例说明如下.

例 8.1.1 (西摩松定理) 从任意一点 D 向任一三角形 ABC 的三边作三条垂线，那么三个垂足 P,Q,R 共线当且仅当 D 点在 $\triangle ABC$ 的外接圆上 (图 5).

考虑定理中"当"的部分. 不失一般性，我们选取以 AB 为横坐标轴、AB 的中垂线为纵坐标轴的笛卡尔坐标系.

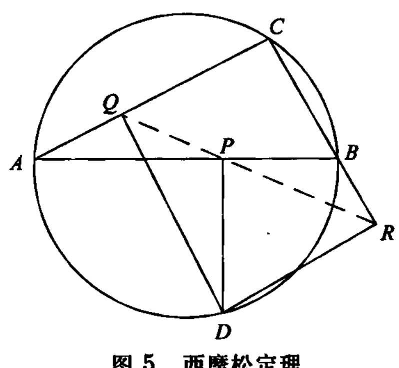


图 5 西摩松定理

设各点的坐标如下：

$$A(-x_1,0),\quad B(x_1,0),\quad C(x_2,x_3),\quad D(x_4,x_5),$$
$$P(x_4,0),\quad Q(x_6,x_7),\quad R(x_8,x_9).$$

定理的假设 HYP 由下列关系组成：

- D 点在 $\triangle ABC$ 的外接圆上

$$\Longleftrightarrow H_1 = x_1x_3x_5^2 - x_1\left(x_3^2+x_2^2-x_1^2\right)x_5 + x_1x_3\left(x_4^2-x_1^2\right)=0;$$

- Q 是 D 点到直线 AC 的垂足

$$\Longleftrightarrow \begin{cases} H_2 = (x_2+x_1)(x_6-x_4)+x_3(x_7-x_5)=0, \\ H_3 = (x_2+x_1)x_7 - x_3(x_6+x_1)=0; \end{cases}$$

- R 是 D 点到直线 BC 的垂足

$$\Longleftrightarrow \begin{cases} H_4 = (x_2-x_1)(x_8-x_4)+x_3(x_9-x_5)=0, \\ H_5 = (x_2-x_1)x_9 - x_3(x_8-x_1)=0. \end{cases}$$

由于 P 点坐标的特殊选取，以下条件自动满足：

- P 是 D 点到直线 AB 的垂足.

细心的读者也许会发现，若三角形 ABC 变为扁平的，则该定理失去意义. 可用下述条件排除这一退化情形：

- 三点 A,B,C 不共线 $\Longleftrightarrow D_1 = x_1x_3 \neq 0$.

排除该退化情形不是实质性的. 我们将会看到，用吴方法可以自动发现 *非退化条件*. 需要证明的定理的结论 CON 为：

- 三点 P,Q,R 共线

$$\Longleftrightarrow G = (x_6-x_4)x_9 - x_7(x_8-x_4)=0.$$

大部分常用的几何关系如共线、垂直和全合的代数表达都只牵涉到多项式方程. 这是吴文俊的灼见，它对几何定理机器证明的理论和方法具有特殊意义. 也因为如此，我们能局限于考虑重要的一类定理，称为 *等式型定理*，它们的代数表示只牵涉到多项式方程和不等方程. 这类定理足以覆盖大量非凡有趣的几何定理，尽管一些牵涉到次序关系的定理被排除在外.

注 8.1.1 如吴文俊在 [96] 的导言中所指出，从几何的公理系统出发到达代数化和坐标化的过程是颇为艰难曲折的. 所幸的是，对通常的欧氏几何我们不是必须经历这一艰难的过程. 原因是我们可以运用有关实数系统的知识和解析几何的标准技巧. 也正因为如此，可以假定我们已知如何像解析几何中那样引进坐标系将常用几何关系翻译为代数表达式，而不必考虑代数化的正确性证明.

例 8.1.1 中表述的西摩松定理是等式型的. 可是，用所给的代数表述我们有可能无法证明逻辑蕴涵 (HYP $\Rightarrow$ CON). 这是由于几何定理的叙述常常隐含着一种假设：所考虑的图形处于 *一般* 位置. 例如，在说到三角形时，我们是指没有退化为一条直线或一个点的真正三角形. 在上面的表述中，这一退化情形已被 *先验地* 排除在外，但其他退化情形有可能仍然包括在内因而使蕴涵 (HYP $\Rightarrow$ CON) 逻辑上不成立. 所以，我们必须确定合适的附加 (非退化) 条件使定理在这些条件之下成立. 这里我们不精确定义 *退化情形* 和 *非退化条件*. 实际上，由于几何定理叙述的不严密性以及“退化”这一词的不同解释，给出这两个概念的定义也相当困难. 我们暂时只要求读者对退化这个概念有一粗略印象，稍后再对此予以解释.

用 $\wedge$, $\vee$ 和 $\Rightarrow$ 分别表示逻辑上的“和”,“或”和“蕴涵”. 我们对几何定理的判定问题提出如下代数表述.

表述 α. 给定一种几何 $\mathfrak{G}$, 特征为 0 的几何附属数域 $\mathcal{K}$ 和一个适当的坐标系 $\mathfrak{O}$, 在此之下可以建立 $\mathfrak{G}$ 中的语句与 $\mathcal{K}$ 上的代数表达式之间的对应. 设 $\mathfrak{G}$ 中定理 $\mathbb{T}$ 的假设在 $\mathfrak{O}$ 之下表示为一组有限多个多项式方程和不等方程

$$\text{HYP:} \quad \begin{cases} H_1(\boldsymbol{x}) = 0, \cdots, H_s(\boldsymbol{x}) = 0, \\ D_1(\boldsymbol{x}) \neq 0, \cdots, D_t(\boldsymbol{x}) \neq 0 \end{cases} \tag{8.1.1}$$

(这里每个 $D_i = 0$ 通常对应于一个通过对定理的分析或考察而 *预先* 确定的退化情形), 而定理的结论则表示为单个多项式方程

$$\text{CON:} \quad G(\boldsymbol{x}) = 0. \tag{8.1.2}$$

所有多项式都是关于变元 $\boldsymbol{x} = (x_1, \cdots, x_n)$ —— 它们是点的坐标和定理中所出现的其他几何量 —— 其系数在 $\mathcal{K}$ 中.

(a) 判定逻辑公式

$$(\forall \boldsymbol{x})\, [H_1(\boldsymbol{x}) = 0 \wedge \cdots \wedge H_s(\boldsymbol{x}) = 0 \wedge D_1(\boldsymbol{x}) \neq 0 \wedge \cdots \wedge D_t(\boldsymbol{x}) \neq 0 \\ \Longrightarrow G(\boldsymbol{x}) = 0] \tag{8.1.3}$$

是否在 $\mathcal{K}$ 或 $\mathcal{K}$ 的某一扩域上成立；如果不是，则

(b) 求出“适当的”附加条件 $D_1^*(\boldsymbol{x}) \neq 0, \cdots, D_{t^*}^*(\boldsymbol{x}) \neq 0$, 使得公式

$$(\forall \boldsymbol{x})\,[H_1(\boldsymbol{x}) = 0 \wedge \cdots \wedge H_s(\boldsymbol{x}) = 0 \wedge D_1(\boldsymbol{x}) \neq 0 \wedge \cdots \wedge D_t(\boldsymbol{x}) \neq 0 \\ \wedge D_1^*(\boldsymbol{x}) \neq 0 \wedge \cdots \wedge D_{t^*}^*(\boldsymbol{x}) \neq 0 \Longrightarrow G(\boldsymbol{x}) = 0]$$

在 $\mathcal{K}$ 或其某一扩域上成立.

确定附加不等方程 $D_j^*(\boldsymbol{x}) \neq 0$ 是为了保证几何假设的构形处于一般位置. 在下述证明算法中，我们置

$$\mathbb{P} = \{H_1, \cdots, H_s\}, \quad \mathbb{Q} = \{D_1, \cdots, D_t\}.$$

对任意几何命题或定理 $\mathbb{T}$, 我们用

- HC($\mathbb{T}$) 表示“$\mathbb{T}$ 的假设自相矛盾”;
- NC($\mathbb{T}$) 表示“$\mathbb{T}$ 未能确认”;
- True($\mathbb{T}$)/SC 表示“$\mathbb{T}$ 在附加条件 SC 之下成立”.

附加条件有可能不明确给出；此时 SC 不置任何值. 若 SC $= \emptyset$, 则定理 $\mathbb{T}$ *普遍*成立；否则，$\mathbb{T}$ 有*条件地*成立.

遵照吴方法[95, 96]的基本原理，我们可以设计出如下简单算法，它对确认几何定理，特别是在使用近特征列和主三角系统时，非常有效.

算法 ProverA: HC, True/SC 或 NC ← ProverA($\mathbb{P}, \mathbb{Q}, G$). 任给一代数形式的等式型几何定理 $\mathbb{T}$: $\mathbb{P} = 0 \wedge \mathbb{Q} \neq 0 \Rightarrow G = 0$, 本算法或者证明 True($\mathbb{T}$)/SC, 或者指出 HC($\mathbb{T}$), 或者告知 NC($\mathbb{T}$).

P1. 用 CharSetN 或 PriTriSys 计算 $\mathbb{P}$ 在 $\mathcal{K}$ 上的 (拟、弱) 中间列 $\mathbb{T}$. 若 $\mathbb{T}$ 为矛盾列或 $0 \in \mathrm{prem}(\mathbb{Q}, \mathbb{T})$, 则指出 HC($\mathbb{T}$), 且算法终止.

P2. 计算 $R \leftarrow \mathrm{prem}(G, \mathbb{T})$. 若 $R \equiv 0$, 则设 $I_1, \cdots, I_r$ 为 $\mathrm{ini}(\mathbb{T})$ 中多项式的所有互异且不整除任何 D_i 的不可约因子，命

$$\mathrm{SC} \leftarrow I_1 \neq 0 \wedge \cdots \wedge I_r \neq 0,$$

且输出 True($\mathbb{T}$)/SC; 否则，告知 NC($\mathbb{T}$).

上面的 P1 和 P2 可以用下列步骤来替代，其中前两步用到了格罗布讷基 (参阅 [47]).

P1′. 计算 $\mathbb{P}\cup\{D_1z_1-1,\cdots,D_tz_t-1\}$ 在 $\mathcal{K}$ 上由 $x_1\prec\cdots\prec x_n\prec z_1\prec\cdots\prec z_t$ 决定的纯字典项序格罗布讷基 $\mathbb{G}$, 这里 $z_1,\cdots,z_t$ 为新未定元. 若 $1\in\mathbb{G}$, 则指出 HC($\mathbb{T}$), 且算法终止.

P2′. 计算 $R\leftarrow\mathrm{rem}(G,\mathbb{G})$. 若 $R\equiv 0$, 则输出 True($\mathbb{T}$)/$\emptyset$, 且算法终止.

P3′. 选取 $\mathbb{G}$ 的拟基列: $\mathbb{B}\leftarrow\mathrm{BasSet}(\mathbb{G})$, 并计算 $R\leftarrow\mathrm{prem}(R,\mathbb{B})$. 若 $R\equiv 0$, 则设 $I_1,\cdots,I_r$ 为 $\mathrm{ini}(\mathbb{B})$ 中多项式的所有互异且不整除任何 D_i 的不可约因子, 命

$$\mathrm{SC}\leftarrow I_1\neq 0\wedge\cdots\wedge I_r\neq 0,$$

且输出 True($\mathbb{T}$)/SC; 否则, 告知 NC($\mathbb{T}$).

该算法以及后几节中所给算法的终止性都是明显的, 因此我们只需证明它们的正确性.

证 由于 CharSetN 或 PriTriSys 计算的 $\mathbb{P}$ 之中间列 $\mathbb{T}$ 包含于 $\mathrm{Ideal}(\mathbb{P})$, 所以 $\mathbb{P}=0$ 意味着 $\mathbb{T}=0$. 设 $\bar{\boldsymbol{x}}\in\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$, 则在 $\mathcal{K}$ 的某一扩域中存在 $\bar{z}_i$, 使得 $D_i(\bar{\boldsymbol{x}})\bar{z}_i-1=0$, $1\leq i\leq t$. 因此对任意

$$F\in\mathbb{G}\cap\mathcal{K}[\boldsymbol{x}]\subset\mathrm{Ideal}(\mathbb{P}\cup\{D_1z_1-1,\cdots,D_tz_t-1\})$$

都有 $F(\bar{\boldsymbol{x}})=0$; 于是 $\mathbb{P}=0$ 和 $\mathbb{Q}\neq 0$ 蕴涵着 $\mathbb{G}\cap\mathcal{K}[\boldsymbol{x}]=0$. 故在

$$\mathrm{rem}(G,\mathbb{G})=\mathrm{rem}(G,\mathbb{G}\cap\mathcal{K}[\boldsymbol{x}])\equiv 0$$

时定理 $\mathbb{T}$ 普遍成立. 根据伪余公式, 若 $R=\mathrm{prem}(G,\mathbb{T})\equiv 0$, 则

$$\mathbb{T}=0\wedge\mathrm{ini}(\mathbb{T})\neq 0\Longrightarrow G=0;$$

这在用 $\mathbb{B}$ 替换 $\mathbb{T}$ 之后也成立. 注意 $\mathbb{B}\subset\mathbb{G}$. 所以, 在 $R\equiv 0$ 时 $\mathbb{T}$ 有条件地成立, 其附加条件为 SC. □

ProverA 中的中间列 $\mathbb{T}$ 也可以是 $\mathbb{F}$ 修正的, 此时 $F=0$ ($F\in\mathbb{F}$) 的情形需要另加处理. 下列步骤对实施几何定理证明器是必要的, 但我们未将其并入本章中所描述的算法.

P0. 这是预处理, 它将定理的几何叙述翻译为代数形式. 这一步可以通过编制一个常用几何关系的翻译器来自动完成.

P∞. 这是后处理，它将所得代数附加条件翻译为几何语句，并确定哪些条件为非退化条件. 在大多数情形，这种翻译也能自动完成 (见如 [14, 86]). 一个附加条件是否为非退化条件可以从其几何意义或通过维数分析等来确定.

大多数几何定理都只在附加条件之下成立，这是吴文俊的卓见. 没有预先确定所有附加条件，步骤 P1′ 和 P2′ 只能证明很有限的定理. 将非退化条件添入假设对于用格罗布讷基来证明几何定理是一个很好的策略. 因此我们应该在表述几何定理的过程中尽量找出非退化条件. 然而，在实际操作时先验地确定所有可能的附加条件使几何定理的叙述严格化是不现实的；将所有那些条件纳入其中也会使定理的假设变得冗长，因而导致较高的计算复杂性.

为了有效地处理附加条件和谈论一般性，我们可以将变元 $\boldsymbol{x}$ 分为 *参量* 和 *几何依量*. 前者是自由变元，能取任意值，而后者则受到几何条件的约束. 如果几何定理的叙述是一步一步、构造性的，变元的区分则相当容易. 假定已将所有参量 $\boldsymbol{u}$ 从 $\boldsymbol{x}$ 中正确地区分开来. 那么 $\boldsymbol{u}$ 的任一不等方程都可以视为非退化条件. 这时，中间列、主三角系统或格罗布讷基都可以在 $\mathcal{K}(\boldsymbol{u})$ 上 (即只对几何依量) 计算. 因此可以证明几何定理在某些非退化条件之下成立，而那些条件并不一定明确给出；此外在使用格罗布讷基时步骤 P3′ 可以省略 (参见 [47]).

定理在某一退化情形是否成立可以用同样的方法来确定，此时只需将退化条件当做定理的又一假设.

除非另有说明，本章以及下一章例子中提到的格罗布讷基都总是对所给变元序决定的纯字典项序而言. 为效率起见，我们也可以选取其他消元项序. 在有些情形，全幂项序就足够了.

例 8.1.2 参见例 8.1.1, 且令 $\mathbb{P}=\{H_1,\cdots,H_5\}$. 关于序 $x_1\prec\cdots\prec x_9$, $\mathbb{P}$ 的弱近特征列为

$$\mathbb{C}=\begin{bmatrix} I_1x_5^2-x_1\left(x_3^2+x_2^2-x_1^2\right)x_5+x_1x_3\left(x_4^2-x_1^2\right), \\ I_2x_6-I_3x_3x_5-I_3^2x_4+x_1x_3^2, \\ I_3x_7-x_3\left(x_6+x_1\right), \\ I_4x_8-I_5x_3x_5-I_5^2x_4-x_1x_3^2, \\ I_5x_9-x_3\left(x_8-x_1\right) \end{bmatrix},$$

其中

$$I_1=x_1x_3,\qquad I_2=x_3^2+I_3^2,\qquad I_3=x_2+x_1,$$
$$I_4=x_3^2+I_5^2,\quad I_5=x_2-x_1$$

分别为 $\mathbb{C}$ 中 5 个多项式 $C_1,\cdots,C_5$ 的初式. 显然 $\text{prem}(I_i,\mathbb{C})$ 对所有 $1\leq i\leq 5$ 都非零，并且 $\text{prem}(D_1,\mathbb{C})$ 也是如此. 容易验证 $\text{prem}(G,\mathbb{C})=0$, 所以定理被证明在附加条件 $I_i\neq 0$ $(2\leq i\leq 5)$ 之下成立. 这些条件的几何意义 —— 由 GEOTHER[86] 自动翻译得出 —— 如下:

- $I_2\neq 0 \Longleftrightarrow AC$ 非迷向;
- $I_3\neq 0 \Longleftrightarrow AC$ 与 AB 不垂直;
- $I_4\neq 0 \Longleftrightarrow BC$ 非迷向;
- $I_5\neq 0 \Longleftrightarrow AB$ 与 BC 不垂直.

我们可以将 $I_i=0$ 作为新假设来检查定理在每一退化情形是否成立. 譬如, 考虑 $I_3=0$ 的情形. 令

$$\mathbb{P}^*=\{H_1,\cdots,H_5,I_3\}.$$

这时, 定理的假设则由 $\mathbb{P}^*=0$ 和 $D_1\neq 0$ 组成. $\mathbb{P}^*$ 在同一变元序下的特征列为

$$\mathbb{C}^*=\left[\begin{array}{l}x_2+x_1,\\ x_5^2-x_3x_5+x_4^2-x_1^2,\\ x_6+x_1,\\ x_7-x_5,\\ (x_3^2+4\,x_1^2)\,x_8+2\,x_1x_3x_5-4\,x_1^2x_4-x_1x_3^2,\\ (x_3^2+4\,x_1^2)\,x_9-x_3^2x_5+2\,x_1x_3x_4-2\,x_1^2x_3\end{array}\right]$$

(计算过程中抹去了一些 x_1 和 x_3 的因子). 因 $\text{prem}(G,\mathbb{C}^*)=0$, 故定理此时在非退化条件 $x_3^2+4x_1^2\neq 0$ (即直线 BC 非迷向) 之下仍然成立.

我们可以按同样方式逐一检查其他退化情形. 下节中将要介绍的系统处理方法是计算 $[\mathbb{P},\{x_1,x_3\}]$ 的零点分解, 以确定对哪些分支定理的结论成立. 最后的结论应该是: 只有第一和第三个非退化条件是必要的.

$\mathbb{P}$ 在相同变元序下的格罗布讷基 $\mathbb{G}$ 由 17 个多项式组成, 而 $\text{rem}(G,\mathbb{G})=G\neq 0$. 现在 $\mathbb{G}$ 的拟基列与 $\mathbb{C}$ 几乎恒同 (只是某些多项式有符号上的差异). 依据上面的验证, 定理被证明在非退化条件 $I_2\cdots I_5\neq 0$ 之下成立.

对于序 $x_5\prec\cdots\prec x_9$, $\mathbb{P}$ 的格罗布讷基为

$$\mathbb{G}^*=[C_1/x_1,C_2,G_3,C_4,G_5],$$

这里

$$G_3 = I_2x_7 - x_3^2x_5 - I_3x_3(x_4 + x_1),$$
$$G_5 = I_4x_9 - x_3^2x_5 - I_5x_3(x_4 - x_1),$$

$C_1, C_2, C_4, I_2, \cdots, I_4$ 同上. 容易验证 $\mathrm{rem}(x_1x_3, \mathbb{G}^*) \neq 0$, 而 $\mathrm{rem}(G, \mathbb{G}^*) = 0$. 由此可见，定理在某些非退化条件之下成立.

上述方法及其变形已由多位学者实施 (见 [14, 43, 45, 92, 95]). 使用不同的证明器已经获得了大量几何定理的机器证明，这些定理包括在 8.3 节中将要介绍的 (广义) 史坦纳定理，摩勒三分角线定理以及最近确认的泰博猜想；同时也发现了一些有意思的“新”定理 (参阅 [95, 96, 14, 85] 和 8.4 节).

8.2 完整方法

必须指出，表述 α 是不够完美的. 首先，我们没有要求在判定 (8.1.3) 的真伪之前检查假设 HYP 的相容性. 如果某个 H_i 比如说是非零常数，那么 $H_i = 0$ 本身就是矛盾的. 这时，公式 (8.1.3) 总是成立. 其次，我们也没有给出所谓“适当”和“附加条件”的定义. 很明显，将 $D_j^* \neq 0$ 添入 HYP 应该不排除定理有意思的情形. 特别每个 $D_j^* = 0$ 都不应该是 HYP 的推论，即将 $D_j^* \neq 0$ 加入 HYP 不会损坏假设的相容性. 然而，完全地检查假设的相容性并强制欲求的附加条件满足上述要求无论理论上还是计算上都不容易.

在证明几何定理的范畴内，发现非退化条件的目的是排除使定理不成立或失去意义的某些退化情形. 这是为了让我们能够有效地证明定理，尽管定理的代数表述因缺少这些条件而逻辑上不一定完全. 丢失非退化条件的原因乃人们表述几何问题的不精确性和几何公理系统的不严密性. 在具体实践时，我们可以通过添加条件来去掉某些退化情形，但要预先确定所有这样的情形则是困难的，甚至是不可能的.

尽管非退化条件已被考虑在内，按表述 α 来证明几何定理我们仍会遇到麻烦. 原因是：将几何语句翻译为代数表达式时，某些对应于几何构形的可约性、模棱两可的情形可能出现. 让我们来看下面的例子.

例 8.2.1 任意三角形三角的平分线三三交于四点.

设该三角形为 $\triangle ABC$, $\angle A$ 和 $\angle B$ 的平分线相交于 D 点，而 $\angle C$ 的平分线与直线 AB 交于 E 点. 我们需要证明 D 在 CE 上.

为了简化计算并且不失一般性，我们将点的坐标选为

$$A(x_1, 0), \quad B(x_2, 0), \quad C(0, x_3), \quad D(x_4, x_5), \quad E(x_6, 0).$$

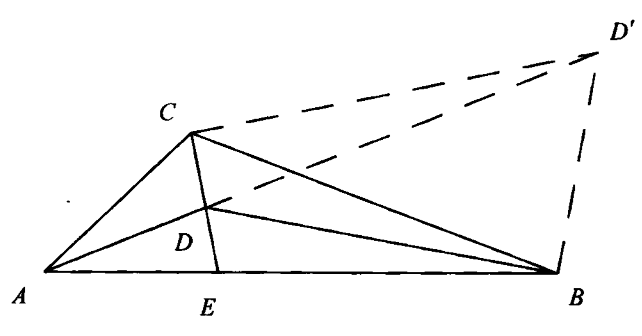


图 6　内旁心定理

定理的假设由下列关系组成:

$$\text{HYP:}\quad\begin{cases} H_1 = x_3\,[x_5^2 - (x_4 - x_1)^2] - 2\,x_1x_5\,(x_4 - x_1) = 0, \\ \qquad\qquad \twoheadleftarrow DA \text{ 是 } \angle CAB \text{ 的平分线} \\ H_2 = x_3\,[x_5^2 - (x_4 - x_2)^2] - 2\,x_2x_5\,(x_4 - x_2) = 0, \\ \qquad\qquad \twoheadleftarrow DB \text{ 是 } \angle ABC \text{ 的平分线} \\ H_3 = x_3\,[(x_1 - x_6)\,(x_3^2 + x_2x_6) + (x_2 - x_6)\,(x_3^2 + x_1x_6)] = 0. \\ \qquad\qquad \twoheadleftarrow EC \text{ 是 } \angle BCA \text{ 的平分线} \end{cases}$$

这里, 角正切的相等用来表示角的全等. 我们用条件

$$D_1 = x_3 \neq 0, \qquad\qquad \twoheadleftarrow C \text{ 不在 } AB \text{ 上}$$

来除去这一平凡的退化情形. 要证明的结论是

$$\text{CON:}\quad G = x_3x_4 + x_5x_6 - x_3x_6 = 0. \quad \twoheadleftarrow D \text{ 在 } CE \text{ 上}$$

乍一看, 我们也许不会发现以上表述有何问题. 仔细考察该定理及其表述, 我们会意识到分角线可以是内分也可以是外分; 两条分角线都由同样的多项式方程来表示. 不用不等式, 我们无法将两种分角线区分开来. 如果 $\triangle ABC$ 一个角的平分线是外分角线而另外两个角的平分线是内分角线, 那么这三条分角线必定不共点. 因此, 用上面的表述不可能证明该定理一般成立. 为了处理这种情形, 让我们对表述稍作修改 (参阅 [96] 194 至 197 页).

例 8.2.2 我们可以不证 D, C, E 共线, 而是证明

$$\text{CON}^*:\quad \begin{aligned} G^* = \quad & [x_1\,(x_5 - x_3) + x_3x_4]\,[x_3\,(x_5 - x_3) - x_2x_4] \\ + \; & [x_2\,(x_5 - x_3) + x_3x_4]\,[x_3\,(x_5 - x_3) - x_1x_4] = 0. \\ & \qquad \twoheadleftarrow DC \text{ 是 } \angle BCA \text{ 的平分线} \end{aligned}$$

这时不需要引进 E 点，而且例 8.2.1 中的第三个关系式 $H_3=0$ 变成多余的. 现在三条分角线不共点的四种可能性已被排除.

在表述其他几何关系如三分角线和两圆相切时也必然会遇到这种模棱两可的情形，我们可用不等式对其予以处理. 如果只用代数方程和不等方程来描述 (无序) 几何定理的假设，上述模棱两可则导致假设所定义的拟代数簇 $\mathcal{V}$ 可约. 若使用定理的自然表述而未将非退化条件和模棱两可性考虑在内，定理的结论通常只对 $\mathcal{V}$ 的某些分支成立. 因此必须去掉那些使定理不成立的分支. 这些分支或者相当于退化情形，或者是由代数表述无法区分的模棱两可所引起的，它们都不是我们需要的情形.

尽管有处理可约性的各种特殊技巧 (参见如 [99, 92])，系统完全地解决这一问题的方法是将 $\mathcal{V}$ 分解为不可约分支.

表述 β. 设 $\mathfrak{G}$, $\mathcal{K}$ 和 $\mathfrak{D}$ 与表述 α 中相同. 又设 $\mathfrak{G}$ 中定理 $\mathbb{T}$ 的假设在 $\mathfrak{D}$ 之下表示为一组有限多个多项式方程和不等方程 (8.1.1)，而其结论表示为单个多项式方程 (8.1.2). 令 $\mathbb{P}=\{H_1,\cdots,H_s\}$, $\mathbb{Q}=\{D_1,\cdots,D_t\}$. 判定

(a) 是否 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})=\emptyset$; 如果不是，

(b) 在 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 的哪些分支上 G 恒为零 (因此 $\mathbb{T}$ 成立).

为明确起见，设 Ψ 为 $[\mathbb{P},\mathbb{Q}]$ 的正则序列，并定义 $[\mathbb{P},\mathbb{Q}]$ 的正则零点集为

$$\mathrm{RegZero}(\mathbb{P}/\mathbb{Q})\triangleq\bigcup_{\mathfrak{T}\in\Psi}\mathrm{RegZero}(\mathfrak{T}),$$

那么问题 (b) 在于将 $\mathrm{RegZero}(\mathbb{P}/\mathbb{Q})$ 分为

$$\mathcal{Z}^+=\{\boldsymbol{\xi}\in\mathrm{RegZero}(\mathbb{P}/\mathbb{Q}):\ G(\boldsymbol{\xi})=0\}\ \text{和}$$
$$\mathcal{Z}^-=\{\boldsymbol{\xi}\in\mathrm{RegZero}(\mathbb{P}/\mathbb{Q}):\ G(\boldsymbol{\xi})\neq0\}.$$

定理 $\mathbb{T}$ 普遍成立当且仅当 $\mathcal{Z}^-=\emptyset$ 而 $\mathcal{Z}^+\neq\emptyset$. 若 $\mathcal{Z}^+=\emptyset$ 但 $\mathcal{Z}^-\neq\emptyset$, 我们说 "$\mathbb{T}$ 一般不成立", 记作 False($\mathbb{T}$). 否则，$\mathbb{T}$ 有条件地成立. 附加条件 SC 可以通过排除 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 的那些使 $\mathbb{T}$ 一般不成立的分支而得出.

以下算法是针对表述 β 设计的.

算法 ProverB: HC, True/SC 或 False $\leftarrow$ ProverB($\mathbb{P},\mathbb{Q},G$). 任给代数化的等式型几何定理 $\mathbb{T}$: $\mathbb{P}=0\wedge\mathbb{Q}\neq0\Rightarrow G=0$, 本算法或者证明 True($\mathbb{T}$)/SC, 或者确定 False($\mathbb{T}$), 或者指出 HC($\mathbb{T}$).

P1. 用 CharSer, TriSer 或 TriSerS 计算 $[\mathbb{P},\mathbb{Q}]$ 在 $\mathcal{K}$ 上的特征序列或三角序列 Ψ. 若 $\Psi=\emptyset$, 则指出 HC($\mathbb{T}$), 且算法终止.

P2. 设 Ψ 中的所有三角系统为 $[\mathbb{T}_1,\mathbb{U}_1],\cdots,[\mathbb{T}_e,\mathbb{U}_e]$. 计算

$$R_i \leftarrow \mathrm{prem}(G,\mathbb{T}_i),\quad 1\le i\le e,$$

且命

$$\Delta \leftarrow \{i\colon\ R_i\ne 0, 1\le i\le e\},\quad \mathcal{Z}\leftarrow \bigcup_{\substack{1\le i\le e\\ i\notin\Delta}} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i).$$

若 $\Delta=\emptyset$, 则

$$\begin{cases} \text{在 } \mathcal{Z}=\emptyset \text{ 时指出 HC}(\mathbb{T}),\\ \text{否则输出 True}(\mathbb{T})/\emptyset, \end{cases}$$

且算法终止.

P3. 对每个 $i\in\Delta$ 用 IrrTriSer, IrrCharSer 或 IrrCharSerE 计算 $[\mathbb{T}_i,\mathbb{U}_i]$ 在 $\mathcal{K}$ 上的不可约三角序列 Ψ_i, 且命 $\Psi^*\leftarrow\bigcup_{i\in\Delta}\Psi_i$. 若 $\Psi^*=\emptyset$, 则

$$\begin{cases} \text{在 } |\Delta|=e \text{ 或 } \mathcal{Z}=\emptyset \text{ 时指出 HC}(\mathbb{T}),\\ \text{否则输出 True}(\mathbb{T})/\emptyset, \end{cases}$$

且算法终止.

P4. 设 $[\mathbb{T}_1^*,\mathbb{U}_1^*],\cdots,[\mathbb{T}_{e^*}^*,\mathbb{U}_{e^*}^*]$ 为 Ψ^* 中的所有不可约三角系统. 计算

$$R_j^*\leftarrow \mathrm{prem}(G,\mathbb{T}_j^*),\quad 1\le j\le e^*,$$

且命 $\Delta^*\leftarrow\{j\colon\ R_j^*\ne 0, 1\le j\le e^*\}$.

若 $\Delta^*=\emptyset$, 则输出 True($\mathbb{T}$)/$\emptyset$, 且算法终止.

若 $|\Delta|=e$ 或 $\mathcal{Z}=\emptyset$, 且 $|\Delta^*|=e^*$, 则输出 False($\mathbb{T}$), 而算法终止.

P5. 命

$$\mathrm{SC}\leftarrow \bigwedge_{j\in\Delta^*}\left(\bigvee_{T\in\mathbb{T}_j^*} T\ne 0 \vee \bigvee_{I\in\mathrm{ini}(\mathbb{T}_j^*)\setminus\mathbb{Q}} I=0\right),$$

且输出 True($\mathbb{T}$)/SC.

证 三角序列 Ψ 和 Ψ^* 给出零点分解

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \mathcal{Z} \cup \mathcal{Z}^+ \cup \mathcal{Z}^-,$$

使得

$$\mathcal{Z} \cup \mathcal{Z}^+ \subset \mathrm{Zero}(G);$$
$$G(\boldsymbol{\xi}) \neq 0, \quad \forall \boldsymbol{\xi} \in \mathcal{Z}^-, \ \boldsymbol{\xi} \text{ 正则},$$

这里

$$\mathcal{Z}^+ = \bigcup_{\substack{1 \leq j \leq e^* \\ j \notin \Delta^*}} \mathrm{Zero}(\mathbb{T}_j^*/\mathbb{U}_j^*), \quad \mathcal{Z}^- = \bigcup_{j \in \Delta^*} \mathrm{Zero}(\mathbb{T}_j^*/\mathbb{U}_j^*).$$

注意，对任意 $1 \leq j \leq e^*$, $\mathbb{T}_j^*$ 都是不可约的. 因此,

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset \iff \mathcal{Z} = \emptyset \ \text{ 且 } \ \Psi^* = \emptyset.$$

假设 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) \neq \emptyset$, 则定理普遍成立, 即 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) \subset \mathrm{Zero}(G)$, 当且仅当 $\Delta^* = \emptyset$. 定理一般不成立当且仅当 $|\Delta| = e$ 或 $\mathcal{Z} = \emptyset$, 且 $|\Delta^*| = e^*$. 否则, 定理有条件地成立, 其附加条件为 SC (参见定理 4.5.11 (b)). □

注 8.2.1 为了提高 ProverB 的实际效率, 一些多余的三角系统, 譬如满足 $|\mathbb{T}| > |\mathbb{P}|$ 的那些 $[\mathbb{T}, \mathbb{U}]$, 应该从 Ψ 和 Ψ_i 中抹去 (见引理 6.2.9). 以上算法首先计算三角序列, 而不是不可约三角序列, 主要是为了绕过不必要的 (代数) 因子分解. 若直接计算 $[\mathbb{P}, \mathbb{Q}]$ 的不可约三角序列, 则能将算法简化. 如果参量 $\boldsymbol{u}$ 已从变元 $\boldsymbol{x}$ 中正确地区分开来而且只需对非退化情形来考虑定理, 那么算法中三角序列的计算也可以在 $\mathcal{K}(\boldsymbol{u})$ 上进行.

对于确认定理, 我们也可以使用反驳法来证明假设关系与结论方程的否定不相容. 在下面的算法 ProverC 中, 所计算的是 $[\mathbb{P}, \mathbb{Q} \cup \{G\}]$ 的不可约 (投影) 三角序列. 为简单起见, 假定 $x_1, \cdots, x_d$ 为参量, 而 $x_{d+1}, \cdots, x_n$ 为几何依量, 并且其区分完全正确. 我们将 SC 加上横杠, 表示附加条件已被确定为非退化条件. 因此, $\mathtt{True}(\mathbb{T})/\overline{\mathrm{SC}}$ 是指 “定理 $\mathbb{T}$ 在非退化条件 $\overline{\mathrm{SC}}$ 之下 一般 成立”. 而且, 我们可以谈论 “$\mathbb{T}$ 不是 一般 成立”, 记作 $\mathtt{NGT}(\mathbb{T})$. 它的意思是, 在 $\mathcal{K}(\boldsymbol{x}_d)$ 的某一代数扩域中存在 $\bar{x}_{d+1}, \cdots, \bar{x}_n$, 使得 $(\boldsymbol{x}_d, \bar{x}_{d+1}, \cdots, \bar{x}_n)$ 为 $[\mathbb{P}, \mathbb{Q}]$ 的零点, 但不是 G 的零点.

算法 ProverC: $\mathtt{HC}$, $\mathtt{True}/\overline{\mathrm{SC}}$ 或 $\mathtt{NGT} \leftarrow \mathrm{ProverC}(\mathbb{P}, \mathbb{Q}, G)$. 任给一代数化的等式型几何定理 $\mathbb{T}$: $\mathbb{P} = 0 \wedge \mathbb{Q} \neq 0 \Rightarrow G = 0$, 本算法或者证明 $\mathtt{True}(\mathbb{T})/\overline{\mathrm{SC}}$, 或者确定 $\mathtt{NGT}(\mathbb{T})$, 或者指出 $\mathtt{HC}(\mathbb{T})$.

P1. 用算法 RegSer, SimSer, TriSerP, IrrCharSer, IrrCharSerE 或 IrrTriSer 确定在 $\bar{\mathcal{K}}$ 中是否 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$. 若是，则指出 $\mathtt{HC}(\mathbb{T})$, 且算法终止.

P2. 用 TriSerP 对 $x_n, \cdots, x_d$ 投影计算 $[\mathbb{P}, \mathbb{Q} \cup \{G\}]$ 在 $\mathcal{K}$ 上的三角序列 Ψ, 或者用 IrrCharSer, IrrCharSerE 或 IrrTriSer 计算 $[\mathbb{P}, \mathbb{Q} \cup \{G\}]$ 在 $\mathcal{K}$ 上的不可约三角序列 Ψ.

若 $\Psi = \emptyset$, 则输出 $\mathtt{True}(\mathbb{T})/\emptyset$, 且算法终止.

设 $[\mathbb{T}_1, \mathbb{U}_1], \cdots, [\mathbb{T}_e, \mathbb{U}_e]$ 为 Ψ 中的所有三角系统. 若对所有 $1 \le i \le e$ 都有 $\mathbb{T}_i^{(d)} \neq \emptyset$, 则设 D_i^* 为 $\mathbb{T}_i^{(d)}$ 中任一多项式，命

$$\overline{\mathrm{SC}} \leftarrow \bigwedge_{i=1}^{e} D_i^* \neq 0,$$

且输出 $\mathtt{True}(\mathbb{T})/\overline{\mathrm{SC}}$; 否则，输出 $\mathtt{NGT}(\mathbb{T})$.

证 若 $\Psi = \emptyset$, 则 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q} \cup \{G\}) = \emptyset$. 由此可见

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) \subset \mathrm{Zero}(G),$$

因而定理普遍成立. 若对所有 $1 \le i \le e$ 都有 $\mathbb{T}_i^{(d)} \neq \emptyset$, 则由 D_i^* 的选取可知

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q} \cup \{D_1^*, \cdots, D_e^*, G\}) = \emptyset.$$

这就意味着

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q} \cup \{D_1^*, \cdots, D_e^*\}) \subset \mathrm{Zero}(G).$$

于是定理有条件地成立，其附加条件为 $\overline{\mathrm{SC}}$. 否则，存在 i, $1 \le i \le e$, 使得 $\mathbb{T}_i^{(d)} = \emptyset$. 注意，$[\mathbb{T}_i, \mathbb{U}_i]$ 是完美的，因此有正则或一般零点 $\boldsymbol{\xi}$. 这时

$$\boldsymbol{\xi} \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q} \cup \{G\}),$$

即 $\boldsymbol{\xi}$ 是 $[\mathbb{P}, \mathbb{Q}]$ 的零点，但不是 G 的零点. 所以定理不是一般成立. □

作为替代，我们也可以按照定理 6.3.3 (c) 通过计算格罗布讷基来确定 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 是否为空集以及使得 $[\mathbb{P}, \mathbb{Q} \cup \{G\}]$ 无零点的附加条件 (参阅 [37, 38, 93]). 这与 ProverA 形成对比：那里假设多项式组的格罗布讷基直接用来将结论多项式约化为 0.

算法 ProverD. 该算法的说明与 ProverA 中相同.

P1. 计算

$$\{H_1, \cdots, H_s, D_1z_1 - 1, \cdots, D_tz_t - 1\}$$

在 $\mathcal{K}$ 上关于任意变元序与容许项序的格罗布讷基 $\mathbb{G}_0$, 这里 $z_1, \cdots, z_t$ 为新未定元. 若 $1 \in \mathbb{G}_0$, 则指出 HC($\mathbb{T}$), 且算法终止.

P2. 计算 $\mathbb{G}_0 \cup \{Gz-1\}$ 在 $\mathcal{K}$ 上关于 $x_1 \prec \cdots \prec x_n \prec z_1 \prec \cdots \prec z_t \prec z$ 的纯字典项序格罗布讷基 $\mathbb{G}$, 这里 z 为另一新变元. 若 $1 \in \mathbb{G}$, 则输出 True($\mathbb{T}$)/$\emptyset$, 且算法终止.

P3. 对每个 $D \in \mathbb{G}$ 执行如下步骤:

若 $D \in \mathcal{K}[\boldsymbol{x}_d]$ 但 $D \notin \{H_1, \cdots, H_s\}$, 则

计算

$$\{H_1, \cdots, H_s, D_1z_1 - 1, \cdots, D_tz_t - 1, Dz - 1\}$$

在任意变元序和容许项序下的格罗布讷基 $\mathbb{G}^*$. 若 $1 \notin \mathbb{G}^*$, 则命 $\overline{\mathrm{SC}} \leftarrow D \neq 0$, 输出 True($\mathbb{T}$)/$\overline{\mathrm{SC}}$, 且算法终止.

P4. 告知 NC($\mathbb{T}$).

算法 ProverC 和 ProverD 的欠缺在于步骤 P1 中额外的相容性验证. 因此实施时应将步骤 P1 和 P2 中的计算结合起来.

8.3 举 例

示范

本小节中我们用例 8.2.1 和 8.2.2 中的表述以及史坦纳定理来说明用前节所给算法证明几何定理的不同方面.

例 8.3.1 见例 8.2.1 和 8.2.2. 确定如下代数形式的定理何时成立:

$$(\forall x_1, \cdots, x_5)\,[H_1 = 0 \wedge H_2 = 0 \wedge D_1 \neq 0 \Longrightarrow G^* = 0].$$

使用 ProverA

计算 $\mathbb{P} = \{H_1, H_2\}$ 关于序 $x_1 \prec \cdots \prec x_5$ 的特征列:

$$\mathbb{C} = [D_1^* x_3 C_1, D_1^* C_2],$$

其中

$$C_1 = 4\,x_4^4 - 8\,\bar{D}x_4^3 - 4\,(x_3^2 - x_1x_2 - \bar{D}^2)\,x_4^2 + 4\,\bar{D}\,(x_3^2 - x_1x_2)\,x_4 - \bar{D}^2x_3^2,$$
$$C_2 = 2\,D_2^*x_5 - x_3\,(2\,x_4 - x_2 - x_1),$$

而

$$D_1^* = x_2 - x_1,\quad D_2^* = x_4 - x_2 - x_1,\quad \bar{D} = x_2 + x_1.$$

$\mathbb{C}$ 中两个多项式的初式分别为

$$I_1 = 4\,D_1^*x_3,\quad I_2 = 2\,D_1^*D_2^*.$$

简单计算表明 $\mathrm{prem}(G^*, \mathbb{C}) = 0$. 因此，我们证明了定理在附加条件 $D_1^* \neq 0$ 和 $D_2^* \neq 0$ 之下成立. 第一个条件有明显的几何意义: A 和 B 不重合; 该附加条件可作为非退化条件.

欲知定理在 $D_2^* = 0$ 时是否成立，我们将假设多项式组扩大为 $\mathbb{P}^* = \mathbb{P} \cup \{D_2^*\}$. 按同样方式，我们能证明此时定理在非退化条件 $D_1^* \neq 0$ 之下也成立.

以上证明没有检查假设的相容性. 若要检查，我们需看是否

$$\mathrm{Zero}(\mathbb{P}/x_3D_1^*D_2^*) = \mathrm{Zero}(\mathbb{C}/x_3D_1^*D_2^*) = \emptyset.$$

使用 ProverB

现在，我们不是对退化情形逐一检验而是计算 $[\mathbb{P}, \{x_3\}]$ 的特征序列以便确定定理何时成立. 对同样的变元序，欲求的序列由如下三个升列组成:

$$\begin{aligned}
\mathbb{C}_1 &= [C_1, C_2],\\
\mathbb{C}_2 &= [D_1^*, C_2'],\\
\mathbb{C}_3 &= [x_2^2 - x_1^2, D_2^*, x_3x_5^2 - 2\,x_1x_2x_5 - x_1^2x_3],
\end{aligned}$$

这里 C_1, C_2, D_1^*, D_2^* 同上，而

$$C_2' = x_3x_5^2 - 2\,x_1\,(x_4 - x_1)\,x_5 - x_3\,(x_4 - x_1)^2.$$

因 $\mathrm{prem}(G^*, \mathbb{C}_1) = 0$, 故定理对 $\mathbb{C}_1$ 成立. 然而 $\mathrm{prem}(G^*, \mathbb{C}_i) \neq 0$, $i = 2, 3$. 容易验证 $\mathbb{C}_2$ 不可约，而 $\mathbb{C}_3$ 可约. 因此，定理对 $\mathbb{C}_2$ 不成立. 没有进一步的计算我们不知道定理对 $\mathbb{C}_3$ 是否成立.

由于 $\mathrm{Zero}(\mathbb{C}_2/\mathrm{ini}(\mathbb{C}_2) \cup \{x_3\}) \neq \emptyset$, 假设的相容性 (即 $\mathrm{Zero}(\mathbb{P}/x_3) \neq \emptyset$) 显而易见.

若将 $x_2^2 - x_1^2 \in \mathbb{C}_3$ 分解为不可约因子以便计算不可约零点分解，我们可以得到三个不可约升列，其中之一是

$$\mathbb{C}_{3'} = [x_2 + x_1, x_4, x_3x_5^2 + 2\,x_1^2x_5 - x_1^2x_3],$$

而另外两个与 $\mathbb{C}_1$ 和 $\mathbb{C}_2$ 相同. 对于这一分解的计算，因子分解并不需要在代数扩域上进行. 也很容易验证 $\mathrm{prem}(G^*, \mathbb{C}_{3'}) = 0$.

于是我们得出结论：定理假设是相容的，定理在非退化条件

$$x_2 - x_1 \neq 0 \vee C_2' \neq 0$$

之下成立，而在退化情形 $x_2 - x_1 = C_2' = 0$ 定理不成立.

这里用不等方程的析取来表示非退化条件是为了使 $\mathrm{Zero}(\mathbb{P}/x_3)$ 中被排除的 (定理不一定成立的) 部分尽可能小. 为简单起见，我们也可以将 $D_1^* = x_2 - x_1 \neq 0$ 作为非退化条件，但该条件排除了使定理成立的某些退化情形，例如 $x_1 = x_2 = x_4 \neq 0, x_5 = 0$.

依定理 6.2.8, 我们有

$$\mathrm{Zero}(\mathbb{P}/x_3) = \mathrm{Zero}(\mathrm{PB}(\mathbb{C}_1)/x_3) \cup \mathrm{Zero}(\mathrm{PB}(\mathbb{C}_2)/x_3).$$

因此，定理假设所定义的几何构形 —— 拟代数簇 —— 被分解为两个不可约分支. 结论多项式 G 在其中的一个分支上为零，而在另一分支上不为零. 所以定理只对一个分支成立，即在 $\triangle ABC$ 处于一般位置时成立. 另外一个使定理不成立的分支对应于 $\triangle ABC$ 退化的情形.

使用 ProverC

代之 $\mathrm{Zero}(\mathbb{P}/x_3)$, 让我们来计算 $\mathrm{Zero}(\mathbb{P}/x_3G^*)$ 在相同变元序下的 (不可约) 分解：此时可得上面给出的升列 $\mathbb{C}_2$ 以及

$$\mathbb{C}_{3''} = [x_2 - x_1, x_4 - 2\,x_1, x_3x_5^2 - 2\,x_1^2x_5 - x_1^2x_3]$$

和两个多项式

$$\begin{aligned} G_2 &= x_3H\,(x_4 - 2\,x_1)\,[(x_4 - 2\,x_1)\,x_5 - x_3\,(x_4 - x_1)], \\ G_{3''} &= x_1x_3H, \end{aligned}$$

其中 $H = x_3^2 + x_1^2$, 使得

$$\mathrm{Zero}(\mathbb{P}/x_3G^*) = \bigcup_{i=2,3''} \mathrm{Zero}(\mathbb{C}_i/G_i).$$

现在两个升列中都含有 x_2-x_1. 如果假定 $x_2\neq x_1$ 并视其为定理的非退化条件，那么 $\mathrm{Zero}(\mathbb{P}/x_3G^*)$ 变为空集；即 $\mathrm{Zero}(\mathbb{P}/(x_2-x_1)\,x_3G^*)=\emptyset$. 因而定理被证明在已知非退化条件 $x_3\neq 0$ 和所求非退化条件 $x_2-x_1\neq 0$ 之下成立.

例 8.3.2 参见例 8.2.1. 试证

$$(\forall x_1,\cdots,x_6)\,[H_1=0\wedge H_2=0\wedge H_3=0\wedge x_3\neq 0\Longrightarrow G=0].$$

为此，令 $\mathbb{P}=\{H_1,H_2,H_3\}$.

使用 ProverB

关于 $x_1\prec\cdots\prec x_6$, $\mathbb{P}$ 的特征列为 $\mathbb{C}=[C_1,C_2,C_3]$ (两个因子 x_3 和 x_2-x_1 在计算过程中被抹去), 这里

$$C_3=H_3=\bar{D}x_6^2+2\,(x_3^2-x_1x_2)\,x_6-\bar{D}x_3^2,$$

而 $C_1,C_2,\bar{D}$ 与例 8.3.1 中相同. 此时 $\mathrm{prem}(G,\mathbb{C})\neq 0$, 所以定理是否成立无可奉告. 于是有必要确定 $\mathbb{C}$ 是否不可约. 用 9.4 节中介绍的方法不难发现，在扩域 $\mathrm{Q}(x_1,\cdots,x_4)$ 上 —— 这里 x_1,x_2,x_3 是作为超越元添入 Q, 而 x_4 是以 C_1 为添加多项式的代数元 —— C_3 是可约的并可分解因子为

$$C_3\doteq\frac{(\bar{D}x_6+2\,x_4^2-2\,\bar{D}x_4)\,(\bar{D}x_6-2\,x_4^2+2\,\bar{D}x_4+2\,x_3^2-2\,x_1x_2)}{\bar{D}}.\tag{8.3.1}$$

事实上, 直接分解 $[\mathbb{P},\{x_3\}]$ 将导致例 4.4.4 中给出的七个不可约三角列 $\mathbb{T}_1,\cdots,\mathbb{T}_7$. 可以验证 $\mathrm{prem}(G,\mathbb{T}_i)=0$ 对 $i=1,3,5$ 成立，但对其他 i 都不成立.

而且从所得的三角列，我们能将 $[\mathbb{P},\{x_3\}]$ 定义的拟代数簇分解为四个不可约分支. 实际上, 这一分解相当于将 (4.4.9) 中 $\mathbb{T}_3,\mathbb{T}_4,\mathbb{T}_5$ 抹去所得的分解. 因此定理只对相应于 $\mathbb{T}_1$ 的分支成立. 相应于 $\mathbb{T}_2$ 的分支代表了像两条角平分线为内分角线而另一条为外分角线的那种情形；它们根本就不是退化情形. 剩下使定理不成立的两个分支则 (可解释为) 对应于退化情形.

如果将 x_1,x_2,x_3 指定为参量 (以保证 $\triangle ABC$ 为一般三角形) 而 x_4,x_5,x_6 为几何依量，并视 x_1,x_2,x_3 的不等方程为定理的非退化条件，那么不可约分解可以在函数域 $\mathrm{Q}(x_1,x_2,x_3)$ 上计算. 如果希望的话，也可以在计算过程中将不等方程记录下来以便确切给出非退化条件. 在这种情形, 不可约特征序列只含有两个三角列 $\mathbb{T}_1$ 和 $\mathbb{T}_2$; 此时 $\mathrm{prem}(G,\mathbb{T}_1)=0$, 而 $\mathrm{prem}(G,\mathbb{T}_2)\neq 0$. 所以，定理对一个分支一般成立而对另一分支一般不成立，因此定理有条件地成立.

使用 ProverC

计算 $[\mathbb{P},\{x_3,G\}]$ 的不可约特征序列给出一个不可约升列，即例 4.4.4 中的 $\mathbb{T}_2$，以及多项式 $G_2=\bar{D}x_3D_2^*G$，使得

$$\mathrm{Zero}(\mathbb{P}/x_3G)=\mathrm{Zero}(\mathbb{T}_2/G_2)\neq\emptyset.$$

没有进一步的考虑和分析，很难从这一升列来判定定理成立与否. 类似地，如果计算 $\mathbb{P}\cup\{x_3Gz-1\}$ (关于 $x_4\prec x_5\prec x_6\prec z$) 的不可约三角序列，那么该序列只含有一个三角列，即 $\mathbb{T}_2\cup[T_4]$，其中

$$T_4=x_3\,[2\,x_4^2-2\,\bar{D}x_4-x_3^2+x_1x_2]\,z-D_2^*,$$

使得

$$\mathrm{Zero}(\mathbb{P}\cup\{Gz-1\})=\mathrm{Zero}(\mathbb{T}_2\cup[T_4]/\mathrm{ini}(\mathbb{T}_2\cup[T_4])).$$

从这一分解我们也不能得出定理条件成立的结论. 这也是为何 ProverC 被看作不完全的. 也有可能通过分析所得升列如解释其多项式的几何意义来确定该定理条件成立，但一般来说这种分析是困难的.

对于例 8.3.2，可在表述定理时用点的反射来代替分角线以避免代数因子分解 (关于其细节见 [96] 第 196 和 197 页).

上面以及后面的例子应该说明了如下事实：对一给定的几何定理可以有很多种叙述方式和代数表述. 定理的证明方法原则上对定理的任何表述都适用，然而不同的表述可以导致非常不同的证明，因此有不可忽视的实际影响. 合适的代数表述可以极大地减少计算复杂性，使看上去超出了方法适用范围的定理有简单的证明，或者绕过代数算法的某些耗时步骤.

例 8.3.3 (史坦纳定理[82, 85, 105, 106]) 设 ABC', BCA' 和 CAB' 为任意三角形 ABC 三条边上的三个或者都向内或者都向外的等边三角形. 那么三条直线 AA', BB' 和 CC' 共点 (见图 7).

不失一般性，设各点的坐标为

$$A(0,0),\quad B(1,0),\quad C(u_1,u_2),\quad C'(y_1,y_2),\quad B'(y_3,y_4),\quad A'(y_5,y_6).$$

则定理可表述为如下代数形式：

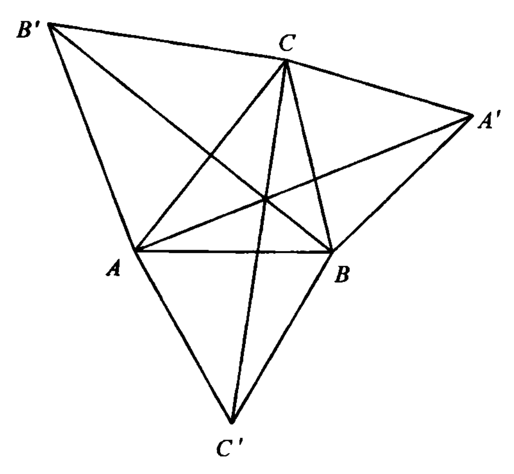


图 7 史坦纳定理

$$\text{HYP:}\quad\begin{cases} H_1 = 2y_1 - 1 = 0, & \twoheadleftarrow\ |AC'| = |BC'| \\ H_2 = y_1^2 + y_2^2 - 1 = 0, & \twoheadleftarrow\ |AC'| = |AB| \\ H_3 = y_3^2 + y_4^2 - u_1^2 - u_2^2 = 0, & \twoheadleftarrow\ |AB'| = |AC| \\ H_4 = y_3^2 + y_4^2 - (y_3 - u_1)^2 \\ \qquad - (y_4 - u_2)^2 = 0, & \twoheadleftarrow\ |AB'| = |CB'| \\ H_5 = (y_5 - 1)^2 + y_6^2 - (u_1 - 1)^2 \\ \qquad - u_2^2 = 0, & \twoheadleftarrow\ |BA'| = |BC| \\ H_6 = (y_5 - 1)^2 + y_6^2 - (y_5 - u_1)^2 \\ \qquad - (y_6 - u_2)^2 = 0, & \twoheadleftarrow\ |BA'| = |CA'| \\ D_1 = u_2 \neq 0, & \twoheadleftarrow\ C \text{ 不在 } AB \text{ 上} \end{cases}$$

$$\text{CON:}\quad\begin{cases} G = (y_1y_4 - u_1y_4 - u_1y_2y_3 + u_2y_1y_3 + u_1y_2 - u_2y_1)\,y_6 \\ \qquad + (u_1y_2 - y_2 - u_2y_1 + u_2)\,y_4y_5 = 0. \\ \qquad\qquad\qquad \twoheadleftarrow\ AA', BB' \text{ 和 } CC' \text{ 共点} \end{cases}$$

这里距离的平方用来代替距离以避免根式，且用 $D_1 \neq 0$ 将 $\triangle ABC$ 退化为一直线的情形排除在外. 变元 u_1, u_2 视为自由参量，而 $y_1, \cdots, y_6$ 为几何依量，它们受代数条件 $H_i = 0\ (1 \leq i \leq 6)$ 的约束.

令

$$\mathbb{P} = \{H_1, \cdots, H_6\},\quad \mathbb{Q} = \{u_2\},\quad \mathbb{Q}^* = \{u_2, G\},$$

且将变元排序为 $u_1 \prec u_2 \prec y_1 \prec \cdots \prec y_6$. 使用 ProverB, 我们计算 Zero($\mathbb{P}/\mathbb{Q}$) 在 Q 上的不可约分解. 算法 IrrTriSer 的输出 Ψ 由 9 个三角

系统 $[\mathbb{T}_i, \mathbb{U}_i]$ 组成, 因此

$$\mathrm{Zero}(\mathbb{P}/u_2) = \bigcup_{i=1}^{9} \mathrm{Zero}(\mathbb{T}_i/u_2), \tag{8.3.2}$$

这里

$$\begin{aligned}
\mathbb{T}_1 &= [T_1, T_2, T_3, T_4, T_5, T_6],\\
\mathbb{T}_2 &= [T_1, T_2, T_3', T_4, T_5', T_6],\\
\mathbb{T}_3 &= [T_1, T_2, T_3', T_4, T_5, T_6],\\
\mathbb{T}_4 &= [T_1, T_2, T_3, T_4, T_5', T_6],\\
\mathbb{T}_5 &= [u_2^2 + u_1^2, T_1, T_2, T_4, T_5, T_6],\\
\mathbb{T}_6 &= [u_2^2 + u_1^2, T_1, T_2, T_4, T_5', T_6],\\
\mathbb{T}_7 &= [u_2^2 + u_1^2 - 2\,u_1 + 1, T_1, T_2, T_3, T_4, T_6],\\
\mathbb{T}_8 &= [u_2^2 + u_1^2 - 2\,u_1 + 1, T_1, T_2, T_3', T_4, T_6],\\
\mathbb{T}_9 &= [2\,u_1 - 1, 4\,u_2^2 + 1, T_1, T_2, T_4, T_6];
\end{aligned}$$

$$\begin{aligned}
T_1 &= 2\,y_1 - 1,\\
T_2 &= 4\,y_2^2 - 3,\\
T_3 &= 2\,y_3 - 2\,u_2 y_2 - u_1,\\
T_3' &= 2\,y_3 + 2\,u_2 y_2 - u_1,\\
T_4 &= 2\,u_2 y_4 + 2\,u_1 y_3 - u_2^2 - u_1^2,\\
T_5 &= 2\,y_5 + 2\,u_2 y_2 - u_1 - 1,\\
T_5' &= 2\,y_5 - 2\,u_2 y_2 - u_1 - 1,\\
T_6 &= 2\,u_2 y_6 + 2\,u_1 y_5 - 2\,y_5 - u_2^2 - u_1^2 + 1.
\end{aligned}$$

于是定理的假设相容. 欲知定理对哪些分支成立, 我们对 $1 \le i \le 9$ 计算 $\mathrm{prem}(G, \mathbb{T}_i)$. 由此发现定理只对 $\mathbb{T}_1$ 成立, 而对所有其他分支都不成立. 所以定理有条件地成立, 其附加条件为

$$\bigwedge_{i=2}^{9} \left(\bigvee_{T \in \mathbb{T}_i} T \neq 0 \right).$$

当定理对 $\mathbb{T}_1$ 而言时, 我们有 $T_1 = \cdots = T_6 = 0$, 而 $u_2 \neq 0$. 因此上述附加条件可简化为

$$T_3' \neq 0 \wedge T_5' \neq 0 \wedge u_2^2 + u_1^2 \neq 0 \wedge u_2^2 + (u_1 - 1)^2 \neq 0.$$

若将变元 u_1 和 u_2 指定为参量，则

$$u_2^2 + u_1^2 \neq 0 \wedge u_2^2 + (u_1 - 1)^2 \neq 0$$

明显是定理的 (极小) 非退化条件，因为它只由 u_1 和 u_2 的多项式不等方程构成．该非退化条件将分支 $\mathbb{T}_5, \cdots, \mathbb{T}_9$ 全部排除．因此，若在 $\mathbb{Q}(u_1, u_2)$ 上计算，前面的分解应变为

$$\text{Zero}(\mathbb{P}/u_2) = \text{Zero}(\mathbb{P}) = \bigcup_{i=1}^{4} \text{Zero}(\mathbb{T}_i).$$

这也可以通过直接计算该分解予以确认．无论从哪种分解，通过验证伪余式我们都能得出定理不是一般成立的结论．

对非退化条件的两个不等方程，不难解释其几何意义：直线 AC 和 BC 都是非迷向的．可是 $T_3' = 0$ 和 $T_5' = 0$ 都不对应于定理的退化情形，因此不能将附加条件 $T_3' \neq 0 \wedge T_5' \neq 0$ 当做非退化条件．仅从这两个多项式来解释该条件的几何意义是不易做到的．

注意 T_3' 和 T_5' 是从 (非退化) 三角列中选来排除不可约分解的三个分支．由于对 u_1 和 u_2 的任意给定值 $y_1, \cdots, y_6$ 对每个分支的值都能从相应的三角列求得，因而每个分支的几何意义可以通过几何手段比如作图来观察获得．这种手段能帮助我们意识到在线段上画三角形的模棱两可性．由此不难发现，$T_3' = 0$ 当且仅当 $\triangle ABC'$ 和 $\triangle CAB'$ 之一是向内画的，而另一个则是向外画的；$T_5' = 0$ 当且仅当 $\triangle ABC'$ 和 $\triangle BCA'$ 之一向内，而另一个向外．定理成立当且仅当 $\triangle ABC', \triangle CAB'$ 和 $\triangle BCA'$ 都向内，或者都向外．

使用 ProverC, 我们计算 $\text{Zero}(\mathbb{P}/\mathbb{Q}^*)$ 在 $\mathbb{Q}$ 上的不可约分解；此时可得 8 个三角列，即上面给出的 $\mathbb{T}_2, \cdots, \mathbb{T}_9$．如果分解在 $\mathbb{Q}(u_1, u_2)$ 上计算，我们则得到三个三角列 $\mathbb{T}_2, \mathbb{T}_3, \mathbb{T}_4$．无论从哪种分解，我们都能获得同样的结论：定理不是一般成立．

上例中史坦纳定理的表述使用了距离的平方，也很直接，因而我们遇到了可约性问题．这是由于线段上的等边三角形画向哪一边不易区分．使用将方向考虑在内的向量旋转，我们可以给如下推广形式的史坦纳定理一个简单表述．用这一表述，机器证明变得相当平凡．

例 8.3.4 (广义史坦纳定理) 设 ABC', BCA' 和 CAB' 为任一三角形 ABC 三边上的三个或者都向内或者都向外的相似等腰三角形，那么三条直线 AA', BB' 和 CC' 共点．

由于 $\triangle ABC'$, $\triangle BCA'$ 和 $\triangle CAB'$ 相似, 它们的高与相应底边 AB, BC 和 CA 的长度成正比. 设其比率为 α, 而六个点的坐标为

$$A(0,0),\ B(x_1,0),\ C(x_2,x_3),\ A'(x_4,x_5),\ B'(x_6,x_7),\ C'(x_8,x_9).$$

为避免可约性问题, 我们将 A' 视为以 B 和 C 的中点为起点、长度为 $\alpha|BC|$ 的向量的终点, 该向量与将 $\overrightarrow{BC}$ 逆时针旋转 $90°$ 所得的向量方向相同. 按这种方式可以类似地构造 B' 和 C'. 于是定理的假设表示为

$$\begin{cases} H_1 = 2x_4 - (x_1 + x_2) + 2\alpha x_3 = 0, \\ H_2 = 2x_5 - x_3 + 2\alpha(x_1 - x_2) = 0, \\ H_3 = 2x_6 - x_2 - 2\alpha x_3 = 0, \\ H_4 = 2x_7 - x_3 + 2\alpha x_2 = 0, \\ H_5 = 2x_8 - x_1 = 0, \\ H_6 = x_9 - \alpha x_1 = 0. \end{cases}$$

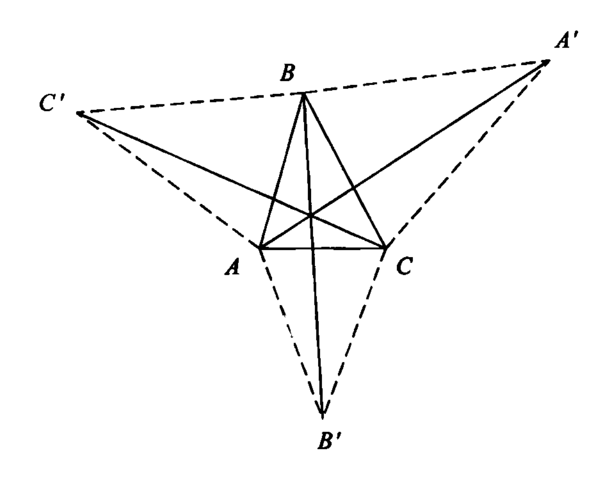


图 8 广义史坦纳定理

关于序 $x_1 \prec x_2 \prec x_3 \prec \alpha \prec x_4 \prec \cdots \prec x_9$ 多项式组 $\mathbb{T} = [H_1, \cdots, H_6]$ 已经是三角列, 并且也是格罗布纳基. 定理的结论为

$$\begin{aligned} G = {} & [(x_2 - x_1)x_4x_7 - x_2x_5(x_6 - x_1)]x_9 + [(x_1x_5 - x_3x_4)x_7 \\ & + x_3x_5(x_6 - x_1)]x_8 - x_1(x_2x_5 - x_3x_4)x_7 = 0. \end{aligned}$$

容易验证 $\mathrm{prem}(G, \mathbb{T}) = \mathrm{rem}(G, \mathbb{T}) \equiv 0$, 且 1 属于 $\mathbb{T} \cup \{Gz - 1\}$ 的格罗布纳基. 因而定理普遍成立.

证例选介

为了展示 8.1 和 8.2 节中所给算法的高效，我们再介绍几个几何定理及其机器证明. 这些定理都很著名，而其证明能在数秒钟内自动完成. 其中有些定理的证明需要用到代数扩域上的多项式因子分解.

我们首先重温初等几何中最优美而又令人惊叹的定理之一 —— 摩勒定理，它是由摩勒在 1899 年前后发现的. 该定理如下推广形式的第一个机器证明由吴文俊[95]给出；吴精心设计了一个巧妙的代数表述. 此后，其他学者相继给出了该定理的 (简化) 机器证明 (参见 [14, 85]).

例 8.3.5 (摩勒定理[14, 85, 95])　任一三角形三角的相邻三分角线相交总共构成 27 个三角形，其中 18 个为等边三角形.

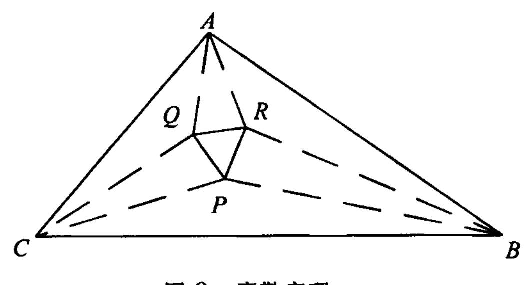


图 9　摩勒定理

遵循吴的表述[95]，定理的假设由下列关系组成：

$$\angle ABC = 3\angle PBC,\quad \angle ACB = 3\angle PCB,\quad \tan^2\theta = 3,$$
$$\angle ABR = \angle PBC,\quad \angle ACQ = \angle PCB,\quad \angle BAR = \angle QAC,$$
$$\angle CBP + \angle PCB + \angle BAR \equiv \theta \bmod 2\pi,$$

而要证的结论为

$$\angle QPR = \angle RQP = \frac{\pi}{3}.$$

置 $x_6 = \tan\theta$，选取各点的坐标如下：

$$A(x_4, x_5),\ B(x_1, 0),\ C(x_2, 0),\ P(0, x_3),\ Q(x_{10}, x_9),\ R(x_8, x_7),$$

并通过取正切来表达角的全等，那么摩勒定理的假设和结论都可以用多项式方程来表示：假设和结论多项式关于变元序 $x_1 \prec \cdots \prec x_{10}$ 的指标三元组分别为

$$[6\ x_5\ 1],\ [6\ x_5\ 1],\ [2\ x_6\ 2],\ [9\ x_8\ 1],\ [9, x_{10}\ 1],\ [41\ x_{10}\ 1],\ [40\ x_8\ 1]$$

和 [9 x_{10} 1], [10 x_{10} 1]. 由此容易用 ProverA 给出定理的证明. 比如, 假设多项式组 (关于 $x_4 \prec \cdots \prec x_{10}$) 的格罗布讷基由 7 个指标三元组为

$$[7\ x_4\ 1],\ [9\ x_5\ 1],\ [2\ x_6\ 2],\ [10\ x_7\ 1],\ [13\ x_8\ 1],\ [10\ x_9\ 1],\ [13\ x_{10}\ 1]$$

的多项式组成. 结论多项式关于该格罗布讷基的余式都为 0. 所以定理在某些可能有的非退化条件之下成立, 而非退化条件没有明确给出.

现在不用吴的技巧, 让我们来考虑定理的自然表述. 这时假设可由下列关系组成:

$$\begin{aligned}&\angle ABC = 3\angle PBC, \quad \angle ACB = 3\angle PCB, \quad \angle CAB = 3\angle RAB,\\ &\angle ABR = \angle PBC, \quad \angle ACQ = \angle PCB, \quad \angle BAR = \angle QAC.\end{aligned}$$

要证的结论是

$$|PQ| = |PR|, \quad |PQ| = |QR|. \tag{8.3.3}$$

将各点的坐标选为

$$A(y_2, y_1),\ B(u_1, 0),\ C(u_2, 0),\ P(0, 1),\ Q(y_6, y_5),\ R(y_4, y_3),$$

那么以上假设和结论都能用多项式方程来表示. 关于变元序 $y_1 \prec \cdots \prec y_6$, 所述多项式的指标三元组为

- 假设: [6 y_2 1], [6 y_2 1], [191 y_4 3], [9 y_4 1], [9 y_6 1], [41 y_6 1];
- 结论: [6 y_6 2], [6 y_6 2].

假设多项式组 $\mathbb{H}$ 在 $\mathbb{Q}(u_1, u_2)$ 上可以分解为两个不可约三角列

$$\mathbb{T} = [T_1, T_2, T_3, T_4, T_5, T_6], \quad \mathbb{T}^* = [T_1, T_2, T_3^*, T_4, T_5, T_6],$$

其中

$$\begin{aligned}
T_1 &= Iy_1 - \alpha\beta,\\
T_2 &= \beta\,(y_2 - u_2) + u_2\,(u_2^2 - 3)\,y_1,\\
T_3 &= Iy_3^2 - 4\,u_1\,(u_1\beta + 4\,u_2)\,y_3 + 4\,u_1^2\beta,\\
T_4 &= 2\,u_1y_4 + (u_1^2 - 1)\,y_3 - 2\,u_1^2,\\
T_5 &= \{[\alpha u_2^3 + u_1^3\beta + (7\,u_1u_2 + 3)\,(u_2 + u_1)]\,y_3 - 2\,u_1\,(u_1^2 + 1)\,\beta\}\,y_5\\
&\quad - 2\,\alpha u_2\,(u_2^2 + 1)\,y_3,\\
T_6 &= (y_2 + u_2y_1 - u_2)\,(y_6 - u_2) - (u_2y_2 - y_1 - u_2^2)\,y_5,\\
T_3^* &= Iy_3 + 2\,u_1\,(u_2 - u_1)\,\beta;
\end{aligned}$$

$$I = \alpha u_2^2 + 8\,u_1u_2 - u_1^2 + 3,$$
$$\alpha = 3\,u_1^2 - 1,\quad \beta = 3\,u_2^2 - 1.$$

以上零点分解的计算不需要代数因子分解. 两个结论多项式对 $\mathbb{T}$ 的伪余式都为 0, 但对 $\mathbb{T}^*$ 的伪余式都不为 0. 因此, 在某些非退化条件之下代数形式的定理对一个分支成立, 而对另一分支不成立.

吴的巧妙表述加上了约束条件

$$\angle CBP + \angle PCB + \angle BAR \equiv \theta \bmod 2\,\pi,$$

这里 $\tan^2\theta = 3$. 将这一条件添入 $\mathbb{H}$ 之后, 分支 $\mathbb{T}^*$ 被排除, 因而只剩下 $\mathbb{T}$. 所以, 在表述时不用吴的技巧我们也能得到同样的结论.

特别指出, 关于 y_3, 多项式 T_3 是二次的而 T_3^* 是一次的. 对此可大致解释如下. 在三角形两角的三分角线固定之后, 第三个角的三分角线有三种可能来构成三角形 PQR. T_3 对应于其中使 $\triangle PQR$ 为等边三角形的两种可能, 而 T_3^* 对应于第三种可能, 对此 $\triangle PQR$ 一般来说不是等边三角形. 为了更清楚地说明前者, 我们引进一个新变元 y_0, 并将 $T_0 = y_0^2 - 3$ 添入 $\mathbb{H}$. 那么在以 T_0 为 y_0 的添加多项式的扩域 $\mathrm{Q}(u_1, u_2, y_0)$ 上 T_3 有形如 (9.4.7) 的因子分解, 因此可将 $\{T_0\} \cup \mathbb{T}$ 进一步分解为两个不可约三角列

$$\mathbb{T}' = [T_0, T_1, T_2, T_3', T_4, T_5, T_6],\quad \mathbb{T}'' = [T_0, T_1, T_2, T_3'', T_4, T_5, T_6].$$

代之 (8.3.3), 我们可以证明结论 $\tan^2\angle QPR = 3$ 和 $\tan^2\angle PQR = 3$; 后者又可写为

$$(\tan\angle QPR + y_0)(\tan\angle QPR - y_0) = 0,$$
$$(\tan\angle PQR + y_0)(\tan\angle PQR - y_0) = 0.$$

容易验证 $\tan\angle QPR + y_0 = 0$ 和 $\tan\angle PQR - y_0 = 0$ 对 $\mathbb{T}'$ 成立, 而 $\tan\angle QPR - y_0 = 0$ 和 $\tan\angle PQR + y_0 = 0$ 对 $\mathbb{T}''$ 成立. 也就是说, 对按 T_3 的两种可能来构成 $\triangle PQR$ 的两个分支定理都成立.

通过多项式因子分解, 也可以将 $\mathbb{H}$ 在 $\mathrm{Q}(u_1, u_2)$ 上分解为两个格罗布纳基 $\mathbb{G}_1$ 和 $\mathbb{G}_2$, 使得

$$\mathrm{Zero}(\mathbb{H}) = \mathrm{Zero}(\mathbb{G}_1) \cup \mathrm{Zero}(\mathbb{G}_2),$$

其中

$$\mathbb{G}_1 = \begin{bmatrix} T_1, G_2, T_3, T_4, \\ u_1cy_5 + au_2y_3 - 2\,u_1u_2\,(u_2 + u_1), \\ 2\,u_1cy_6 - ady_3 + 2\,u_1\,(u_1d - 2\,u_2) \end{bmatrix},$$

$$\mathbb{G}_2 = \begin{bmatrix} T_1, G_2, T_3^*, \\ Iy_4 - 3\,bu_2^3 - 2\,u_1c - 7\,u_1^2u_2 - u_2, \\ Iy_5 - 2\,\alpha u_2\,(u_2 - u_1), \\ Iy_6 - 3\,u_1^3d - 7\,u_1u_2^2 - 2\,au_2 - u_1 \end{bmatrix};$$

$$G_2 = Iy_2 - 8\,u_1u_2\,(u_2 + u_1);$$

$$a = u_1^2 + 1, \quad b = u_1^2 - 1, \quad c = u_2^2 + 1, \quad d = u_2^2 - 1.$$

容易验证，两个结论多项式对 $\mathbb{G}_2$ 的余式都为 0, 但对 $\mathbb{G}_1$ 的余式都不为 0. 因此，在某些非退化条件之下定理对一个分支成立，而对另一分支不成立. 这正好反映了 27 个三角形中 18 个是等边三角形而另外 9 个不是这一事实.

例 8.3.6 (泰博 - 泰勒定理[14, 85, 99, 105, 106]) 给定任意三角形 ABC 以及 BC 边上的一点 D, 并设 C_2 为任一与 $\triangle ABC$ 的外接圆 C_0 以及直线 AD 和 BC 都相切的 (泰博) 圆，其圆心为 T, 那么在 $\triangle ABC$ 的内切和外切圆中恰有一圆 C_1, 其圆心为 I, 使得 TI 经过另一与 C_0 和 AD, BC 都相切的泰博圆 C_3 的圆心.

我们使用文献 [106] 中给出的代数表述，其中假设多项式组 $\mathbb{H}$ 由 7 个关于变元 $u_1 \prec u_2 \prec u_3 \prec x_1 \prec \cdots \prec x_7$ 且指标三元组为

$$[11\ x_1\ 2],\quad [35\ x_2\ 2],\quad [35\ x_3\ 2],\quad [3\ x_4\ 1],\quad [3\ x_5\ 1],\quad [12\ x_6\ 1],\quad [13\ x_7\ 1]$$

的多项式构成，而结论为单个多项式方程 $G = 0$; G 的指标三元组为 $[11\ x_7\ 1]$. $\mathbb{H}$ 在 $\mathrm{Q}(u_1, u_2, u_3)$ 上可以分解为四个不可约三角列 $\mathbb{T}_i$:

$$\mathbb{T}_1 = [T_1, T_2, T_3, T_4, \cdots, T_7], \quad \mathbb{T}_3 = [T_1, T_2', T_3, T_4, \cdots, T_7],$$
$$\mathbb{T}_2 = [T_1, T_2, T_3', T_4, \cdots, T_7], \quad \mathbb{T}_4 = [T_1, T_2', T_3', T_4, \cdots, T_7];$$

$$\begin{aligned}
T_1 &= 4\,u_1^2u_2^4x_1^2 - (2\,u_2^2u_3 - \gamma + 2\,u_1^2u_2^2)\,(2\,u_1^2u_2^2u_3 + u_1^2\gamma - 2\,u_2^2),\\
T_2 &= 2\,u_2adx_2 + 2\,u_1u_2\alpha\,(x_1 + u_3) + \delta,\\
T_3 &= 2\,u_2adx_3 - 2\,u_1u_2\alpha\,(x_1 - u_3) + \delta,\\
T_4 &= u_1u_2x_4 - ab,\\
T_5 &= u_1u_2x_5 - cd,\\
T_6 &= 2\,u_1^2\,[u_2^2\,(x_5 + x_4) - \beta]\,x_6 - u_1^2\gamma\,(x_5 + x_4) + \beta\,(u_1^4 + 1),\\
T_7 &= abcdx_7 + [2\,u_1^2u_2^2x_5 + cd\,(u_1^2u_2^2 + 1)]\,x_6 - u_1^2\gamma x_5 + u_2^4 - u_1^4,\\
T_2' &= 2\,u_2bcx_2 - 2\,u_1u_2\alpha\,(x_1 + u_3) + \delta,\\
T_3' &= 2\,u_2bcx_3 + 2\,u_1u_2\alpha\,(x_1 - u_3) + \delta;
\end{aligned}$$

$$a=u_1u_2+1,\quad b=u_1u_2-1,\quad c=u_1+u_2,\quad d=u_1-u_2,$$
$$\alpha=u_2^2-1,\quad \beta=u_2^4-1,\quad \gamma=u_2^4+1,\quad \delta=(u_1^2+1)\,\alpha^2.$$

G 对 $\mathbb{T}_1$ 的伪余式为 0, 但对 $\mathbb{T}_2,\mathbb{T}_3$ 和 $\mathbb{T}_4$ 的伪余式都不为 0. 所以, 代数形式的定理对一个分支成立, 而对所有其他分支都不成立. 在证明的约化过程中出现的最大多项式有 168 项. 一半以上的计算时间花在 (9.4.8) 和 (9.4.9) 所示的两个代数因子分解上.

例 8.3.7 (史坦纳 - 勒穆斯定理[104]) 两条内分角线 $|AA'|$ 和 $|BB'|$ 相等的任意三角形 ABC 是等腰三角形.

不失一般性, 设各点的坐标为

$$A(-1,0),\quad B(1,0),\quad C(x_1,x_2),\quad A'(x_3,x_4),\quad B'(x_5,x_6).$$

定理的假设由下列关系组成:

$$\begin{cases} H_1=x_2x_4^2+2\,(x_1+1)\,(x_3+1)\,x_4 & \\ \qquad -\;x_2\,(x_3+1)^2=0, & \twoheadleftarrow\ \angle CAA'=\angle A'AB \\ H_2=x_2x_6^2+2\,(x_1-1)\,(x_5-1)\,x_6 & \\ \qquad -\;x_2\,(x_5-1)^2=0, & \twoheadleftarrow\ \angle ABB'=\angle B'BC \\ H_3=(x_1+1)\,x_6-x_2\,(x_5+1)=0, & \twoheadleftarrow\ B'\ 在\ AC\ 上 \\ H_4=(x_1-1)\,x_4-x_2\,(x_3-1)=0, & \twoheadleftarrow\ A'\ 在\ BC\ 上 \\ H_5=x_6^2+(x_5-1)^2-x_4^2 & \\ \qquad -\;(x_3+1)^2=0. & \twoheadleftarrow\ |AA'|=|BB'| \end{cases}$$

我们现在的问题是决定何时 $G=x_1=0$, 即 $|AC|=|BC|$. 关于序 $x_1\prec\cdots\prec x_6$, 用 IrrCharSer 可将 $\{H_1,\cdots,H_5\}$ 在 Q 上分解为 15 个不可约升列; 若用 IrrTriSer, 则分解为 21 个不可约三角列. 其中 6 个升列含有 x_2; 这些升列对应于 A,B,C 共线这一退化情形. 在剩下的 9 个升列中有 4 个升列以 x_1 为其首项; 因此代数形式的定理对这 4 个分支成立, 而对其他分支都不成立.

在零点分解过程中需要计算好几个代数因子分解. 其中两个将作为 (9.4.10) 和 (9.4.11) 在 9.4 节中给出.

上面的例子说明了代数因子分解在几何定理机器证明中的意义. 此时需要分解的多项式以及添加多项式往往都是二次的. 次数低主要是因为至今所考虑的几何定理都只涉及像三角形和圆这样的图形, 它们的代数特征都不高

于二次. 而且我们经常小心翼翼地将代数表述简化以避免高次多项式. 如果我们在代数表述时漫不经心或者考虑具有高阶代数特征的几何图形, 那么要分解的多项式以及代数扩域的添加多项式的次数都有可能大于 2. 这一点从因子分解 (8.3.1) 和下例可见一斑.

例 8.3.8 (费尔巴哈定理 [96]) 任意三角形的九点圆与该三角形的内、外切圆都相切.

参见 [96] 中 (198 至 202 页) 所给的代数表述. 容易验证, 那里的结论多项式 G 可以在 $\mathbb{Q}$ 上分解为不可约因子, 而假设多项式组在 $\mathbb{Q}(x_1, x_2, x_3)$ 上能分解为四个不可约升列 (无需代数因子分解). 对每个升列, 在 G 的四个因子中有且仅有一个其伪余式恒为 0. 这一现象容易从几何上给予解释. 我们尝试了一种更自然的代数表述, 它与吴的表述不同. 在我们的情形, 假设多项式组也能在相应的有理函数域上分解为四个不可约升列, 并且出现类似的现象. 可是用我们的表述, 在计算不可约零点分解时代数因子分解则必不可少. 其中两个因子分解如 (9.4.3) 和 (9.4.4) 所示.

8.4 发现几何定理

在证明定理时, 有一个已知的结论, 其正确性有待我们确认. 现在考虑另一种情形: 我们事先不知道可能有的结论或几何关系, 但希望推导出这种关系. 我们将举例说明如何用消去法来处理这种情形.

现在已知若干几何量之间的几何假设, 我们希望自动导出其中某些量之间可能存在的未知代数关系. 基本想法是: 先将几何假设代数化以得到一组多项式方程和不等方程, 再对适当的变元序计算相应多项式组或系统的特征列、三角序列或格罗布讷基, 最后从三角化的多项式组获得欲求的未知关系. 一个典型的例子是秦九韶 - 海伦公式 (用三角形的三边表示该三角形的面积) 的自动推导 (见例 8.4.1).

推导未知代数关系问题及其解答可叙述为如下形式的算法.

算法 Discover: HC, NO 或 $R \leftarrow$ Discover($\mathbb{P}, \mathbb{Q}$). 给定一组几何假设 HYP, 它表示为一组以几何量 $\boldsymbol{u} = (u_1, \cdots, u_d)$ 与 $\boldsymbol{x} = (x_1, \cdots, x_n)$ 为变元、系数在 $\mathcal{K}$ 中的多项式方程和不等方程

$$\mathbb{P} = \{P_1(\boldsymbol{u}, \boldsymbol{x}), \cdots, P_s(\boldsymbol{u}, \boldsymbol{x})\} = 0,$$
$$\mathbb{Q} = \{Q_1(\boldsymbol{u}, \boldsymbol{x}), \cdots, Q_t(\boldsymbol{u}, \boldsymbol{x})\} \neq 0;$$

又给定一固定整数 k, 不失一般性, 设 $k=1$, 本算法或者指出 HC(HYP), 或者确定在 $\boldsymbol{u}$ 和 x_1 之间是否存在一多项式关系 $R(\boldsymbol{u},x_1)=0$ 使得 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})\subset\mathrm{Zero}(R)$, 若是, 则求出 $R(\boldsymbol{u},x_1)$; 否则, 算法输出 NO.

D1. 在 $\mathcal{K}$ 上用 CharSetN 或 PriTriSys 计算 $\mathbb{P}$ 的 (拟、弱) 中间列 $\mathbb{T}$, 或者计算 $\mathbb{P}\cup\{Q_1z_1-1,\cdots,Q_tz_t-1\}$ 关于 $u_1\prec\cdots\prec u_d\prec x_1\prec\cdots\prec x_n\prec z_1\prec\cdots\prec z_t$ 的纯字典项序格罗布讷基 $\mathbb{T}$, 这里 $z_1,\cdots,z_t$ 为新未定元. 若 $\mathbb{T}\cap\mathcal{K}\neq\emptyset$ 或 $0\in\mathrm{prem}(\mathbb{Q},\mathbb{T})$, 则指出 HC(HYP), 且算法终止.

D2. 命 $\mathbb{T}^{\langle 1\rangle}\leftarrow\mathbb{T}\cap(\mathcal{K}[\boldsymbol{u},x_1]\setminus\mathcal{K}[\boldsymbol{u}])$. 如果 $\mathbb{T}$ 是 D1 中计算的格罗布讷基, 则转至 D4. 如果存在多项式 $R(\boldsymbol{u},x_1)\in\mathbb{T}^{\langle 1\rangle}$ 并且 $\mathbb{T}\cap\mathcal{K}[\boldsymbol{u}]$ 或者是空集或者作为三角列是不可约的, 则输出 $R(\boldsymbol{u},x_1)$, 且算法终止.

D3. 计算 $[\mathbb{P},\mathbb{Q}]$ 在 $\mathcal{K}$ 上的不可约三角序列 $\Psi=\{[\mathbb{T}_1,\mathbb{U}_1],\cdots,[\mathbb{T}_e,\mathbb{U}_e]\}$. 若 $\Psi=\emptyset$, 则指出 HC(HYP), 且算法终止. 命

$$\mathbb{T}_i^{\langle 1\rangle}\leftarrow\mathbb{T}_i\cap(\mathcal{K}[\boldsymbol{u},x_1]\setminus\mathcal{K}[\boldsymbol{u}]),\quad 1\leq i\leq e.$$

如果对每个 $1\leq i\leq e$ 都存在多项式 $R_i(\boldsymbol{u},x_1)\in\mathbb{T}_i^{\langle 1\rangle}$, 则输出

$$R(\boldsymbol{u},x_1)\leftarrow\prod_{i=1}^{e}R_i(\boldsymbol{u},x_1);$$

否则, 输出 NO. 算法终止.

D4. 若 $\mathbb{T}^{\langle 1\rangle}\neq\emptyset$, 则输出关于 x_1 次数最小的多项式 $R(\boldsymbol{u},x_1)\in\mathbb{T}^{\langle 1\rangle}$; 否则, 输出 NO.

证　等式 $R(\boldsymbol{u},x_1)=0$, 若已求得, 则明显是 $\boldsymbol{u}$ 和 x_1 之间的多项式关系. 由于 $\mathbb{T}$ 是 CharSetN 或 PriTriSys 计算的 $\mathbb{P}$ 的中间列, 或者是 $\mathbb{P}^*=\mathbb{P}\cup\{Q_1z_1-1,\cdots,Q_tz_t-1\}$ 的格罗布讷基, 故 $\mathbb{T}\subset\mathrm{Ideal}(\mathbb{P}^*)$. 因此 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})\subset\mathrm{Zero}(R)$.

若存在 i, $1\leq i\leq e$, 使得 $\mathbb{T}_i^{\langle 1\rangle}=\emptyset$, 则 x_1 为 $\mathbb{T}_i$ 的参量. 这时, 对固定的 $\boldsymbol{u}=\bar{\boldsymbol{u}}$, x_1 在 $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ 中的取值范围是 $\mathcal{K}$ 的无穷子集. 所以, 一般来说 $\boldsymbol{u}$ 和 x_1 之间不存在代数关系. 这一结论在 $\mathbb{T}$ 为 $\mathbb{P}^*$ 的格罗布讷基而 $\mathbb{T}^{\langle 1\rangle}=\emptyset$ 时也是正确的. □

可将下面的后处理并入上述算法.

D∞. 在输出 NO 之后，分析所计算的不可约三角序列或格罗布讷基；尝试提供适当的、形如 $D_i \neq 0$ 的附加条件，并将 D_i 添入 $\mathbb{Q}$ 以排除某些分支获得可能的代数关系.

在变元 $\boldsymbol{u}$ 被指定为独立参量时，三角列、三角序列和格罗布讷基也可以在 $\mathbb{Q}(\boldsymbol{u})$ 上计算，即将 $\boldsymbol{u}$ 被多项式方程所约束的情形都作为退化情形. 这时算法或者检测出 $\boldsymbol{u}$ 的代数相关性，或者导出一般成立的代数关系；该关系在退化情形不一定成立.

例 8.4.1 (秦 - 海伦公式 [98, 15, 84]) 求任意三角形 ABC 的面积 Δ 关于其三边 a, b, c 的表达式.

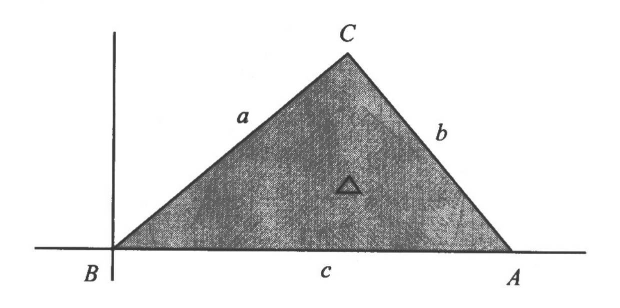


图 10 秦 - 海伦公式

设三角形的顶点分别位于 $A(x_1, 0)$, $B(0,0)$, $C(x_2, x_3)$, 那么几何假设可用下列多项式方程来表示：

$$\text{HYP}: \begin{cases} H_1 = x_1^2 - c^2 = 0, & \leftarrow c = |AB| \\ H_2 = x_2^2 + x_3^2 - a^2 = 0, & \leftarrow a = |BC| \\ H_3 = (x_2 - x_1)^2 + x_3^2 - b^2 = 0, & \leftarrow b = |AC| \\ H_4 = x_3^2 x_1^2 - 4\Delta^2 = 0. & \leftarrow \Delta = \frac{1}{2}|AB| \cdot |x_3| \end{cases}$$

令 $\mathbb{P} = \{H_1, \cdots, H_4\}$, 并将变元排序为 $a \prec b \prec c \prec \Delta \prec x_1 \prec x_2 \prec x_3$. 容易计算 $\mathbb{P}$ 的主三角系统 $[\mathbb{T}, \mathbb{U}]$:

$$\mathbb{T} = [R, H_1, T, H_2], \quad \mathbb{U} = \{x_1\},$$

其中

$$R = 16\,\Delta^2 + c^4 - 2\,b^2c^2 - 2\,a^2c^2 + b^4 - 2\,a^2b^2 + a^4,$$
$$T = 2\,x_1x_2 - c^2 + b^2 - a^2.$$

实际上，$\mathbb{T}$ 是 $\mathbb{P}$ 的弱特征列．$\mathbb{P}$ 的格罗布讷基为

$$\mathbb{G}=[R,H_1,2\,c^2x_2-(c^2-b^2+a^2)\,x_1,T,H_2].$$

无论在哪种情形，$R=0$ 都给出我们要求的代数关系．置 $p=(a+b+c)/2$，则有

$$\Delta^2=p\,(p-a)\,(p-b)\,(p-c).$$

这就是著名的 秦 – 海伦公式[98].

例 8.4.2 (勃拉默高泰公式[15, 84])　求圆内接有向四边形 $ABCD$ 带符号的面积关于其四边的表达式.

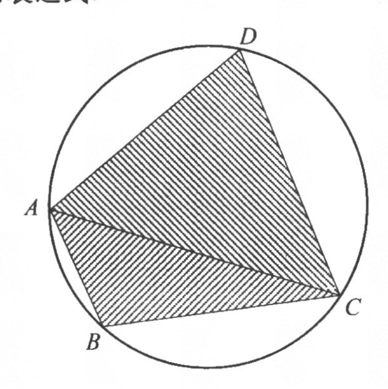


图 11　勃拉默高泰公式

将各点的坐标选为

$$A(0,0),\quad B(a,0),\quad C(x_1,x_2),\quad D(x_3,x_4),$$

且命

$$b=|BC|,\quad c=|CD|,\quad d=|DA|.$$

又用 Θ 表示 $\triangle ABC$ 和 $\triangle ACD$ 带符号的面积之和．那么有关这些几何量的条件可以表示为

$$\begin{cases} H_1=x_2^2+x_1^2-2\,ax_1-b^2+a^2=0,\\ H_2=x_4^2-2\,x_2x_4+x_3^2-2\,x_1x_3+x_2^2+x_1^2-c^2=0,\\ H_3=x_4^2+x_3^2-d^2=0,\\ H_4=ax_2x_4^2-a\,(x_2^2+x_1^2-ax_1)\,x_4+ax_2x_3^2-a^2x_2x_3=0,\\ H_5=x_1x_4-x_2x_3+ax_2-2\,\Theta=0.\end{cases}$$

我们希望求得 $a,\cdots,d$ 和 Θ 之间的关系. 为此, 令 $\mathbb{P}=\{H_1,\cdots,H_5\}$, 并计算 $\mathbb{P}$ 关于序 $a\prec\cdots\prec d\prec\Theta\prec x_1\prec\cdots\prec x_4$ 的拟近特征列 $\mathbb{C}$: 不难发现 $\mathbb{C}$ 含有五个指标三元组为

$$[46\ \Theta\ 4],\quad [35\ x_1\ 1],\quad [6\ x_2\ 1],\quad [10\ x_3\ 1],\quad [4\ x_4\ 1]$$

的多项式, 而在计算过程中抹去的因子为 a,x_1 和 $F=d^2+c^2-b^2-a^2$. 因此, 我们有零点关系

$$\mathrm{Zero}(\mathbb{P}/ax_1F)\subset\mathrm{Zero}(\mathbb{C}).$$

容易检验, $ax_1F=0$ 对应于几何问题的某些退化情形. $\mathbb{C}$ 中的第一个多项式 R 可以分解因子为

$$R=(R_0+8\,abcd)\,(R_0-8\,abcd),$$

其中

$$R_0=16\,\Theta^2+d^4-2\,(c^2+b^2+a^2)\,d^2+c^4-2\,(b^2+a^2)\,c^2+(b^2-a^2)^2.$$

于是, 我们得到在某些非退化条件之下的代数关系 $R=0$. 事实上, 通过计算特征序列我们已经验证 $R=0$ 在所有退化情形都成立; 换言之, 所得关系总是几何假设的推论.

也可以求出 $\mathbb{P}$ 关于 $\Theta\prec x_1\prec\cdots\prec x_4$ 的格罗布纳基, 它由五个指标三元组为

$$[46\ \Theta\ 4],\quad [26\ x_1\ 1],\quad [13\ x_2\ 1],\quad [26\ x_3\ 1],\quad [13\ x_4\ 1]$$

的多项式构成. 其中第一个多项式与上面的 R 相同. 因而用格罗布纳基方法导出同样的关系 $R=0$ 也不困难. 通过计算比如 $\mathbb{H}\cup\{Rz-1\}$ 在 $\mathbf{Q}$ 上关于全幂项序的格罗布纳基也能验证 $R=0$ 普遍成立; 1 属于该格罗布纳基.

置 $p=(a+b+c+d)/2$; $R=0$ 意味着下列等式之一成立:

$$\Theta^2=(p-a)\,(p-b)\,(p-c)\,(p-d),$$
$$\Theta^2=p\,(p-a-b)\,(p-a-c)\,(p-a-d).$$

前者是著名的勃拉默高泰公式, 它在 $a,\cdots,d$ 中正变元的个数 t 为偶数时给出实际结果; 后者在 t 为奇数时给出实际结果 (参见 [15]).

例 8.4.3 考虑例 8.4.2 中的几何问题. 所述定理也可以按如下 (不同) 方式来 "发现". 受秦 - 海伦公式的启发, 我们可以猜测勃拉默高泰公式对任意有向四边形 $ABCD$ 都成立. 换言之, 我们希望证明

$$(\forall a,b,c,d,x_1,\cdots,x_4,\Theta)\,[H_1=0\wedge H_2=0\wedge H_3=0\wedge H_5=0 \\ \Longrightarrow R_0+8\,abcd=0],$$

其中多项式与例 8.4.2 中相同. 这一猜想在 A,B,C,D 中有两点重合时明显成立. 如果它不是对任意 A,B,C,D 都成立, 那么应存在约束这四点的某种关系. 因此我们将变元 $a,x_1,\cdots,x_4$ 之一排在其他变元之首, 例如

$$x_4\prec\Theta\prec b\prec c\prec d.$$

对这一变元序, 容易计算

$$\{H_1,H_2,H_3,H_5,R_0+8\,abcd\}$$

的格罗布讷基 $\mathbb{G}$. 结果发现 $\mathbb{G}$ 中含有多项式 $(H_4/a)^2$. 也就是说,

$$H_1=0,\quad H_2=0,\quad H_3=0,\quad H_5=0,\quad R_0+8\,abcd=0$$

蕴涵着 $H_4=0$. 所以, 上述猜测只能在 $H_4=0$, 即 A,B,C,D 共圆时成立. 当然可以验证, 在 $H_4=0$ 添入假设之后, 猜测的确成立. 这样一来, 我们又重新发现了勃拉默高泰公式.

例 8.4.4 (彭赛列定理) 设 R 为任一三角形外接圆的半径, r 为该三角形内切圆的半径, 而 d 为这两个圆的中心之间的距离. 求 R,r 和 d 之间的关系.

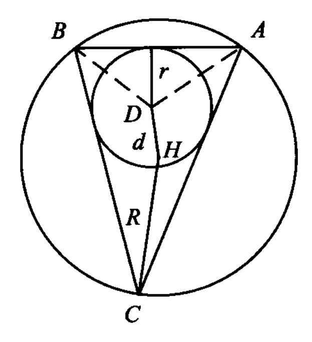


图 12 彭赛列定理

设 ABC 为任意三角形, D 和 H 分别为 $\triangle ABC$ 的内心和外接圆心, 而各点的坐标为

$$A(x_1,0),\ B(x_2,0),\ D(0,x_3),\ C(x_4,x_5),\ H(x_6,x_7).$$

现在几何假设为:

- C 点在 AB 关于 AD 的反射线上

$$\iff H_1=(x_2-x_1)\left[(x_3^2-x_1^2)\,x_5-2\,x_1x_3\,(x_4-x_1)\right]=0;$$

- C 点在 BA 关于 BD 的反射线上

$$\iff H_2=(x_2-x_1)\left[(x_3^2-x_2^2)\,x_5-2\,x_2x_3\,(x_4-x_2)\right]=0;$$

- H 为 $\triangle ABC$ 的外接圆心

$$\iff \begin{cases} H_3=(x_2-x_1)\,(2\,x_6-x_2-x_1)=0, \\ H_4=2\,x_5x_7+2\,x_4x_6-2\,x_2x_6-x_5^2-x_4^2+x_2^2=0; \end{cases}$$

- r 为 $\triangle ABC$ 内切圆的半径 $\Longrightarrow H_5=r^2-x_3^2=0;$
- R 为 $\triangle ABC$ 外接圆的半径 $\Longrightarrow H_6=R^2-x_7^2-(x_6-x_1)^2=0;$
- $d=|DH| \Longrightarrow H_7=d^2-(x_7-x_3)^2-x_6^2=0.$

假定 $\triangle ABC$ 不退化为一直线, 因此 $(x_2-x_1)\,x_5\neq 0$.

计算

$$\{H_1,\cdots,H_7,(x_2-x_1)\,z_1-1,x_5z_2-1\}$$

关于 $d\prec x_2\prec\cdots\prec x_7\prec z_1\prec z_2$ 的格罗布讷基 $\mathbb{G}$, 我们发现 $\mathbb{G}$ 中有一个多项式 G 只含有 d,R,r:

$$G=d^4-2\,d^2R^2+R^4-4\,R^2r^2=(d^2-R^2+2\,Rr)\,(d^2-R^2-2\,Rr).$$

所以, 上述几何假设蕴涵着 $G=0$. 对于上面的推导, 我们并没有用到隐含的假设: $R>0$, $r>0$, $d\geq 0$. 而且, $\triangle ABC$ 的外接圆包含其内切圆, 因此 $R>d$. 于是我们有

$$R^2-2\,Rr=d^2.$$

这正是彭赛列大定理; 它重新由 Discover 自动发现.

通过计算三角列或三角系统 (而不是格罗布讷基) 也容易推导出上面两例中的结果.

第九章　其 他 应 用

本章简述消去法的若干其他应用. 本书的续篇将讨论更广泛的应用问题, 举出各种实例, 并介绍有关软件. 我们鼓励读者运用消去法去解决自己所遇到的理论与实际问题.

9.1 轨迹方程的自动推导

推导公式的方法经适当修改可以用来推导给定几何描述的运动之轨迹方程. 两者的区别在于: 这里我们需要确定 n 个变元 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 与 $\boldsymbol{u}$ 之间一组或几组代数关系, 而且需要用到投影.

说到轨迹方程, 我们是指一组或者几组以 $\boldsymbol{u}$ 为参量、$\boldsymbol{x}$ 的多项式方程和不等方程的析取, 使得不仅该方程组或析取是几何假设的推论, 而且对轨迹上的任意一点都存在至少一个满足该几何假设的构形.

在叙述问题以及给出其算法解答之前, 让我们作如下约定. 对任意集合的并 $S=\bigcup_{A\in\Delta}S_A$, 从 S 中 抹去多余集合 是指确定 Δ 的子集 Δ', 使得 $\bigcup_{A\in\Delta\setminus\Delta'}S_A=S$. 化简 S 的意思是求出另一集合 Ω, 使得 $\bigcup_{A\in\Omega}S_A=S$, 且作为 S 的表示 $\bigcup_{A\in\Omega}S_A$ 比 $\bigcup_{A\in\Delta}S_A$ 简单. 我们已在 6.2 节中指出了一些抹去多余零点集的可能性. 其他技巧见诸于一些有关实施的论文, 如 [16, 83]. 仔细讨论如何化简零点集的并则超出了本节的范围. 关于化简的示范, 见例 9.2.1 和 9.2.2.

算法 Derive: $\Psi\leftarrow\text{Derive}(\mathbb{P},\mathbb{Q})$. 给定一点 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 在 n 维仿射空间 $\mathbf{A}^n_{\mathcal{K}}$ 中运动的几何约束 HYP, 它表示为一组 $\boldsymbol{u},\boldsymbol{x}$ 与 $\boldsymbol{y}$ 的多项式方程和不等方程

$$\mathbb{P}=\{P_1(\boldsymbol{u},\boldsymbol{x},\boldsymbol{y}),\cdots,P_s(\boldsymbol{u},\boldsymbol{x},\boldsymbol{y})\}=0,$$
$$\mathbb{Q}=\{Q_1(\boldsymbol{u},\boldsymbol{x},\boldsymbol{y}),\cdots,Q_t(\boldsymbol{u},\boldsymbol{x},\boldsymbol{y})\}\neq 0,$$

这里 $\boldsymbol{u}=(u_1,\cdots,u_d)$ 是一组 (几何) 参量, 而 $\boldsymbol{y}=(y_1,\cdots,y_m)$ 为一组其他几何量, 本算法计算有限多个 $\mathcal{K}(\boldsymbol{u})[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P}_1,\mathbb{Q}_1],\cdots,[\mathbb{P}_e,\mathbb{Q}_e]$ 构成的集合 Ψ, 使得

(a) 对任意 $(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}})\in\text{Zero}(\mathbb{P}/\mathbb{Q})$, 都存在下标 i, $1\leq i\leq e$, 使得 $\bar{\boldsymbol{x}}\in\text{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$;

(b) 对任意 $1 \le i \le e$ 和 $\bar{\boldsymbol{x}} \in \text{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$, 都存在 $\bar{\boldsymbol{y}} \in \tilde{\mathcal{K}}^m$, 使得

$$(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \in \text{Zero}(\mathbb{P}/\mathbb{Q}).$$

称析取

$$\bigvee_{i=1}^{e} (\mathbb{P}_i = 0 \wedge \mathbb{Q}_i \neq 0)$$

为点 $\boldsymbol{x}$ (于 $\boldsymbol{u}$) 的 *轨迹方程*.

D1. 关于变元序 $x_1 \prec \cdots \prec x_n \prec y_1 \prec \cdots \prec y_m$, 计算 $[\mathbb{P}, \mathbb{Q}]$ 的正则序列 Ψ, 或者对 $\boldsymbol{y}$ 带投影的特征序列、三角序列或纯字典项序格罗布讷序列 Ψ. 若 $\Psi = \emptyset$, 即 $\text{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$, 则或者几何条件自相矛盾, 或者所述运动为自由运动 (即对任意 $\bar{\boldsymbol{x}}$ 都存在 $\bar{\boldsymbol{y}}$, 使得 $(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \in \text{Zero}(\mathbb{P}/\mathbb{Q})$, 因此该运动的轨迹覆盖整个空间); 于是算法终止.

D2. 从

$$\bigcup_{[\mathbb{T},\mathbb{U}]\in\Psi} \text{Zero}(\mathbb{T} \cap \mathcal{K}(\boldsymbol{u})[\boldsymbol{x}]/\mathbb{U} \cap \mathcal{K}(\boldsymbol{u})[\boldsymbol{x}])$$

中抹去多余的集合, 对其化简, 并设所得的零点集为 $\bigcup_{i=1}^{e} \text{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$. 输出

$$\Psi \leftarrow \{[\mathbb{P}_1, \mathbb{Q}_1], \cdots, [\mathbb{P}_e, \mathbb{Q}_e]\}.$$

证 由特征序列、特征序列、三角序列和格罗布讷序列的定义以及 $[\mathbb{T}, \mathbb{U}] \in \Psi$ 的投影性质即得. □

D1 中的序列 Ψ 也可以在 $\mathcal{K}[\boldsymbol{u}, \boldsymbol{x}, \boldsymbol{y}]$ 中计算. 实际上, 我们只需对 $\boldsymbol{y}$ 进行消元; 原因是求出 $\boldsymbol{u}$ 与 $\boldsymbol{x}$ 的方程和不等方程就够了 —— 它们不必是三角化的. 我们不再讨论投影格罗布讷基的技术性细节 (见例 9.2.1).

例 9.1.1 设一平面与四面体 $ABCD$ 的四边 AB, AC, DC, DB 分别交于点 E, F, G, H, 使得 $EFGH$ 为平行四边形. 求 $\square EFGH$ 的中心 O 的轨迹方程.

设各点的坐标为

$$A(0,0,0),\quad B(u_1,0,0),\quad C(u_2,u_3,0),\quad D(u_4,u_5,u_6),\quad E(y_1,0,0),$$
$$F(y_2,y_3,0),\quad G(y_4,y_5,y_6),\quad H(y_7,y_8,y_9),\quad O(X,Y,Z).$$

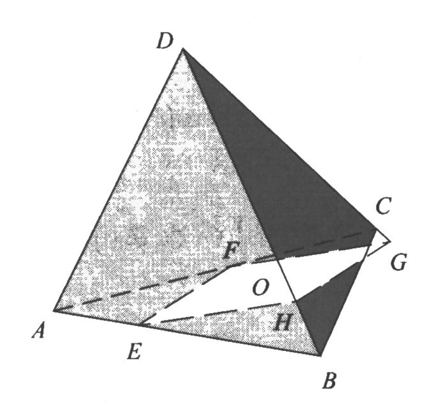


图 13　推导轨迹方程

我们有下列关系：

$$\begin{aligned}
&H_1 = u_2y_3 - u_3y_2 = 0, && \leftarrow F \text{ 在 } AC \text{ 上}\\
&\left.\begin{aligned}&H_2 = u_4y_6 - u_2y_6 - u_6y_4 + u_2u_6 = 0,\\ &H_3 = u_4y_5 - u_2y_5 - u_5y_4 + u_3y_4\\ &\qquad + u_2u_5 - u_3u_4 = 0,\end{aligned}\right\} && \leftarrow G \text{ 在 } CD \text{ 上}\\
&\left.\begin{aligned}&H_4 = u_4y_8 - u_1y_8 - u_5y_7 + u_1u_5 = 0,\\ &H_5 = u_4y_9 - u_1y_9 - u_6y_7 + u_1u_6 = 0,\end{aligned}\right\} && \leftarrow H \text{ 在 } BD \text{ 上}\\
&\left.\begin{aligned}&H_6 = y_7 - y_4 + y_2 - y_1 = 0,\\ &H_7 = y_8 - y_5 + y_3 = 0,\\ &H_8 = y_9 - y_6 = 0,\end{aligned}\right\} && \leftarrow \overrightarrow{FE} = \overrightarrow{GH}\\
&\left.\begin{aligned}&H_9 = 2X - y_4 - y_1 = 0,\\ &H_{10} = 2Y - y_5 = 0,\\ &H_{11} = 2Z - y_6 = 0.\end{aligned}\right\} && \leftarrow O \text{ 为 } \square EFGH \text{ 的中心}
\end{aligned}$$

令 $\mathbb{P} = \{H_1, \cdots, H_{11}\}$, 并将变元排序为

$$X \prec Y \prec Z \prec y_1 \prec \cdots \prec y_9.$$

无论是 $\mathbb{P}$ 的特征序列或三角序列还是 (纯字典项序) 格罗布讷序列都只含有一个元素 (三角系统、升列或格罗布讷基). 将它们的零点集投影到 X, Y, Z, 我们得到 (相同的) 前两个多项式:

$$\begin{aligned}
P_1 &= 2(u_3 - u_5)X - 2(u_1 + u_2 - u_4)Y + (u_1 + u_2)u_5 - u_3u_4,\\
P_2 &= 2u_6X + 2(u_1 + u_2 - u_4)Z - (u_1 + u_2)u_6.
\end{aligned}$$

这是由于所有初式都只含参量 u_i. 所以要求的轨迹方程为 $P_1 = 0 \wedge P_2 = 0$, 它是 $P_1 = 0$ 和 $P_2 = 0$ 分别定义的两个平面的交线.

例 9.1.2 (双弧 [84]) 给定两段不同圆弧上的两点 A 和 B 以及该圆弧在 A, B 处的切线，求一中间点 M —— 在此处两段圆弧相连并有公共切线 —— 的轨迹.

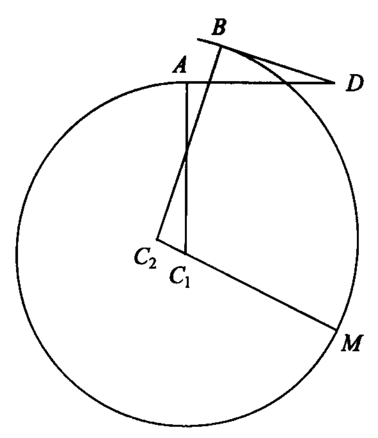


图 14 双弧

本例源自纳特布讷和马丁的著作 [84], 其中著者用技巧性的推导证明了轨迹的一个分支为圆. 这里，我们说明如何用消去法来自动推导要求的轨迹. 现将各点的坐标选为

$$A(0,0),\ \ D(u_1,0),\ \ B(u_2,u_3),\ \ M(X,Y),\ \ C_1(0,x_1),\ \ C_2(x_2,x_3).$$

从已知几何条件我们得到下列关系:

$$\text{HYP:}\quad \begin{cases} H_1 = (u_2-u_1)\,(x_2-u_2) + u_3\,(x_3-u_3) = 0, \\ \qquad\qquad\qquad\qquad\qquad\qquad \twoheadleftarrow\ BC_2 \perp BD \\ H_2 = X^2 + (x_1-Y)^2 - x_1^2 = 0, \qquad \twoheadleftarrow\ |C_1A| = |C_1M| \\ H_3 = (x_2-u_2)^2 + (x_3-u_3)^2 - (x_2-X)^2 \\ \qquad\quad - (x_3-Y)^2 = 0, \qquad\qquad \twoheadleftarrow\ |C_2B| = |C_2M| \\ H_4 = X\,(x_3-x_1) + x_2\,(x_1-Y) = 0. \\ \qquad\qquad\qquad\qquad\qquad\qquad \twoheadleftarrow\ M \text{ 在 } C_1C_2 \text{ 上} \end{cases}$$

命 $\mathbb{P} = \{H_1, \cdots, H_4\}$, 而 $X \prec Y \prec x_1 \prec x_2 \prec x_3$. $\mathbb{P}$ 的特征序列由三个升列组成，其中最复杂者含有

$$\begin{aligned} R = {} & u_3\,(X^2+Y^2)^2 - 2\,u_1u_3X(X^2+Y^2) + 2\,(u_1u_2 - u_2^2 - u_3^2)\,(X^2+Y^2)\,Y \\ & + (2\,u_1u_2 - u_2^2 - u_3^2)\,u_3\,(X^2-Y^2) + 2\,(u_2^3 - u_1u_2^2 + u_2u_3^2 + u_1u_3^2)\,XY \end{aligned}$$

以及另外三个指标三元组为 $[3\ x_1\ 1]$, $[12\ x_2\ 1]$ 和 $[6\ x_3\ 1]$ 的多项式. 两个较简单的升列为

$$[X-u_2, Y-u_3, 2\,u_3x_1-u_3^2-u_2^2, -x_2+u_2, x_3-u_3],$$
$$[X, Y, x_1, [4\ x_2\ 1], [5\ x_3\ 1]].$$

三个升列 (的零点集) 投影到 X, Y 的结果是

$$\{R\},\quad \{X-u_2, Y-u_3\},\quad \{X, Y\}.$$

后两个多项式组分别对应于 B 和 A 点; 它们在曲线 $R=0$ 上, 因此是多余的. 所以, $R=0$ 就是我们要求的 M 点的轨迹方程.

$\mathbb{P}$ 对 x_3, x_2, x_1 带投影的三角序列与上面的特征序列相仿. $\mathbb{P}$ 的格罗布讷基由 R 和另外六个指标三元组为

$$[20\ x_1\ 1],\quad [3\ x_1\ 1],\quad [39\ x_2\ 1],\quad [12\ x_2\ 1],\quad [22\ x_2\ 1],\quad [6\ x_3\ 1]$$

的多项式构成. 通过进一步计算格罗布讷基并进行投影, 我们也能推导出同样的轨迹方程 $R=0$.

使用 FactorA 的扩展 (见 9.4 节以及 [74]), 我们可以将 R 分解为以下两个多项式的乘积:

$$R_1=\left(X-\frac{u_1-\alpha}{2}\right)^2+\left(Y-\frac{\beta+u_2\alpha}{2\,u_3}\right)^2-\frac{\alpha\,(u_1u_2+\beta)}{2\,(u_1-u_2+\alpha)},$$
$$R_2=\left(X-\frac{u_1+\alpha}{2}\right)^2+\left(Y-\frac{\beta-u_2\alpha}{2\,u_3}\right)^2-\frac{\alpha\,(u_1u_2+\beta)}{2\,(u_2-u_1+\alpha)},$$

其中

$$\alpha=\sqrt{u_3^2+(u_1-u_2)^2}=|BD|,$$
$$\beta=u_1u_2-u_1^2+\alpha^2.$$

所以对任意固定的 u_1, u_2 和 u_3, M 点的轨迹有两个分支. $R_1=0$ 和 $R_2=0$ 表示两个经过 A 与 B 的圆 $\odot I_1$ 和 $\odot I_2$, 其圆心 I_1, I_2 和半径都容易确定. 我们曾以为两圆之一对应于凸形双弧, 而另一圆对应于 S 形双弧; 但事实并非如此. 实际情况似乎相当复杂. 在图 15 中我们对特定的 $u_1=-40, u_2=55, u_3=80$ 用数值模拟来观察圆心为 C_1 和 C_2 的两圆 $\odot C_1$ 和 $\odot C_2$ 在 M 点处是如何沿着轨迹圆 $\odot I_1$ 和 $\odot I_2$ 相切的. 圆 $\odot I_1$ 被两条直线 AD 和 BD 分为四段圆弧, 而 $\odot I_2$ 也是如此. $\odot C_1$ 和 $\odot C_2$ 在 M 沿着

$\odot I_1$ 或 $\odot I_2$ 上两段相对的圆弧运动时 外 切, 而在另外情形 内 切. 对于内切的情形, 在 M 沿着两段圆弧之一移动时, $\odot C_1$ 位于 $\odot C_2$ 内部, 而在 M 沿着另一段圆弧移动时, $\odot C_2$ 位于 $\odot C_1$ 内部. 一个遗留下来的有趣几何问题是: 这一结论是否总正确.

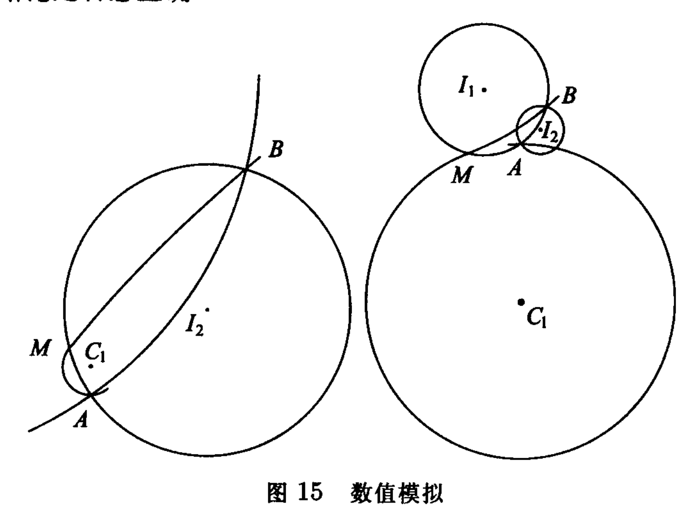


图 15 数值模拟

用以上方法也能建立空间双弧的轨迹方程. 我们略去其细节.

9.2 参数对象的隐式化

几何对象如曲线和曲面的代数表示可以用隐式方程也可以用参数方程. 每种表示的优点取决于所要处理问题的类型. 对于几何造型, 人们经常需要将一种表示转换为另一种表示. 几何对象在 n 维仿射空间中的有理参数化可以表示为

$$x_1 = \frac{P_1(\boldsymbol{y})}{Q_1(\boldsymbol{y})}, \cdots, x_n = \frac{P_n(\boldsymbol{y})}{Q_n(\boldsymbol{y})},$$

这里 $\boldsymbol{y} = (y_1, \cdots, y_m)$ 为参数. 隐式化问题在于求出 $\boldsymbol{x}$ 的隐式方程使其与参数化表示定义相同的几何对象. 下面的算法可以用来解决这一问题. 将投影并入隐式化算法是由李子明 [51] 首先建议的.

算法 Impli: $\Psi \leftarrow \mathrm{Impli}(P_1, \cdots, P_n; Q_1, \cdots, Q_n)$. 给定两组 $\mathcal{K}[\boldsymbol{y}]$ 中的多项式 $P_1, \cdots, P_n$ 和 $Q_1, \cdots, Q_n$, 这里 $Q_1 \cdots Q_n \neq 0$ 且 $m \leq n$, 本算法计算有限多个 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathbb{P}_1, \mathbb{Q}_1], \cdots, [\mathbb{P}_e, \mathbb{Q}_e]$ 构成的集合 Ψ, 使得对

任意 $\bar{\boldsymbol{x}} = (\bar{x}_1, \cdots, \bar{x}_n) \in \tilde{\mathcal{K}}^n$,

$$\bar{\boldsymbol{x}} \in \bigcup_{i=1}^{e} \operatorname{Zero}(\mathbb{P}_i/\mathbb{Q}_i) \iff \begin{cases} \exists\, \bar{\boldsymbol{y}} \in \tilde{\mathcal{K}}^m, \text{ 使得} \\ \bar{x}_1 = \dfrac{P_1(\bar{\boldsymbol{y}})}{Q_1(\bar{\boldsymbol{y}})}, \cdots, \bar{x}_n = \dfrac{P_n(\bar{\boldsymbol{y}})}{Q_n(\bar{\boldsymbol{y}})}. \end{cases}$$

I1. 命

$$\mathbb{P} \leftarrow \{P_1 - x_1Q_1, \cdots, P_n - x_nQ_n\},$$
$$\mathbb{Q} \leftarrow \{Q_1, \cdots, Q_n\},$$
$$\mathbb{P}^* \leftarrow \mathbb{P} \cup \{z_1Q_1 - 1, \cdots, z_nQ_n - 1\},$$

而 $x_1 \prec \cdots \prec x_n \prec y_1 \prec \cdots \prec y_m \prec z_1 \prec \cdots \prec z_n$, 这里 z_j 为新未定元. 计算 $[\mathbb{P}, \mathbb{Q}]$ 的正则序列或对 $z_1, \cdots, z_n$ 和 $\boldsymbol{y}$ 带投影的三角序列 Ψ, 或者 $\mathbb{P}^*$ 在纯字典项序下对 $z_1, \cdots, z_n$ 和 $\boldsymbol{y}$ 带投影的格罗布纳序列 Ψ.

I2. 从 $\bigcup_{[\mathbb{T},\mathbb{U}]\in\Psi} \operatorname{Zero}(\mathbb{T} \cap \mathcal{K}[\boldsymbol{x}]/\mathbb{U} \cap \mathcal{K}[\boldsymbol{x}])$ 中抹去多余的集合, 将其化简, 并设所得的零点集为 $\bigcup_{i=1}^{e} \operatorname{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$. 输出

$$\Psi \leftarrow \{[\mathbb{P}_1, \mathbb{Q}_1], \cdots, [\mathbb{P}_e, \mathbb{Q}_e]\}.$$

证　由正则序列、三角序列和格罗布纳序列的定义以及 $[\mathbb{T}, \mathbb{U}] \in \Psi$ 的投影性质即得. □

例 9.2.1 (参阅 [9, 103, 84])　考虑三维仿射空间中由下列方程定义的参数曲面

$$x = rt, \quad y = rt^2, \quad z = r^2.$$

置 $\mathbb{P} = \{x - rt, y - rt^2, z - r^2\}$. 容易计算 $\mathbb{P}$ 关于 $z \prec y \prec x \prec t \prec r$ 的格罗布纳基

$$\mathbb{G} = [x^4 - zy^2, zyt - x^3, xt - y, zt^2 - x^2, yr - x^2, xr - zt, tr - x, r^2 - z].$$

从 $\mathbb{G}$ 得出的方程 $x^4 - zy^2 = 0$ 似是上述参数曲面的隐式方程, 但如布赫贝格尔在 [9] 中所提到的, 这一方程并不严格符合隐式化问题的要求. 原因是 y 轴乃该方程之解, 可是它并不出现在参数表示所定义的曲面上.

为了使用投影以得到确切的隐式方程, 我们将 x —— 它是 $\mathbb{G}$ 中关于其导元次数最低 (为 1) 的第三和第六个多项式的初式 —— 添入 $\mathbb{P}$, 计算所得多项式组的格罗布纳基, 并如此进行. 最终我们可以得到另外两个格罗布纳基

$$\mathbb{G}_1 = [y, x, t, r^2 - z], \quad \mathbb{G}_2 = [z, y, x, r],$$

使得

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{G}/x) \cup \mathrm{Zero}(\mathbb{G}_1) \cup \mathrm{Zero}(\mathbb{G}_2).$$

于是

$$\begin{aligned}
&\mathrm{Proj}_{z,y,x}\mathrm{Zero}(\mathbb{P}) \\
&\quad = \mathrm{Proj}_{z,y,x}\mathrm{Zero}(\mathbb{G}/x) \cup \mathrm{Proj}_{z,y,x}\mathrm{Zero}(\mathbb{G}_1) \cup \mathrm{Proj}_{z,y,x}\mathrm{Zero}(\mathbb{G}_2) \\
&\quad = \mathrm{Zero}(y^2z - x^4/xyz) \cup \mathrm{Zero}(\{x,y\}) \cup \mathrm{Zero}(\{x,y,z\}) \\
&\quad = \mathrm{Zero}(y^2z - x^4/xy) \cup \mathrm{Zero}(\{x,y\}).
\end{aligned}$$

这就意味着要求的隐式方程为

$$(y^2z - x^4 = 0 \wedge xy \neq 0) \vee (x = 0 \wedge y = 0).$$

现在计算 $\mathbb{P}$ 关于同一变元序的特征序列，该序列由以下三个升列组成:

$$\begin{aligned}
&\mathbb{C}_1 = [x^4 - zy^2, xt - y, yr - x^2], \\
&\mathbb{C}_2 = \mathbb{G}_1, \quad \mathbb{C}_3 = \mathbb{G}_2.
\end{aligned}$$

对它们相应的零点集投影，我们得到同样的隐式方程.

例 9.2.2 求下列方程所定义的曲线 (关于变元 x 和 y) 之隐式表示:

$$\begin{aligned}
&(x-u)^2 + (y-v)^2 - 1 = 0, \\
&v^2 - u^3 = 0, \\
&2v(x-u) + 3u^2(y-v) = 0, \\
&(3wu^2 - 1)(2wv - 1) = 0.
\end{aligned}$$

这是曲线 $y^2 - x^3 = 0$ 支距的一种表述. 我们视 u, v, w 为参数. 以上多项式已在例 3.1.2 中出现; 例 4.2.2 中计算了它们关于变元序 $x \prec y \prec u \prec v \prec w$ 对 w, v, u 带投影的三角序列. 该序列中的五个三角系统 $[\mathbb{T}_i, \mathbb{U}_i]$ 也在例 4.2.2 中列出. 因此，欲求的隐式方程可由

$$\bigvee_{i=1}^{5} (\mathbb{T}_i^{(2)} = 0 \wedge \mathbb{U}_i^{(2)} \neq 0) \tag{9.2.1}$$

给出，这里 $\mathbb{T}_i^{(2)} = \mathbb{T}_i \cap \mathrm{Q}[x,y]$, $\mathbb{U}_i^{(2)} = \mathbb{U}_i \cap \mathrm{Q}[x,y]$, $1 \leq i \leq 5$. 可是方程 (9.2.1) 相当冗长. 现说明如何将其大大简化. 首先计算 $[\mathbb{T}_i^{(2)}, \mathbb{U}_i^{(2)}]$ 的正则序列，我们发现对 $i = 2, \cdots, 5$, $\mathbb{U}_i^{(2)}$ 中的所有多项式都能消去. 换言之,

$$\mathrm{Zero}(\mathbb{T}_i^{(2)}/\mathbb{U}_i^{(2)}) = \mathrm{Zero}(\mathbb{T}_i^{(2)}), \quad 2 \leq i \leq 5.$$

$[\mathbb{T}_1^{(2)}, \mathbb{U}_1^{(2)}]$ 的正则序列由三个正则系统 $[\mathbb{T}_{1j}, \mathbb{U}_{1j}]$ 组成，这里 $\mathbb{T}_{11} = [T_{11}]$，而

$$\begin{aligned}
\mathbb{T}_{12} &= [T_{41}, 729\,y^4 - Hy^2 + \mathrm{coef}(T_{11}, y^2)],\\
\mathbb{T}_{13} &= [T_{31}, 729\,(18\,x-1)\,y^2 - 39366\,x^4 - 26244\,x^3 - 60993\,x^2\\
&\qquad - 32868\,x - 13381],\\
\mathbb{U}_{11} &= \{x, T_{21}, T_{31}, T_{41}\},\quad \mathbb{U}_{12} = \mathbb{U}_{13} = \emptyset.
\end{aligned}$$

关于多项式 H, T_{11}, T_{21} 等，见例 3.1.2 和 4.2.2. 容易验证

$$\begin{aligned}
\mathcal{Z}_1 &= \mathrm{Zero}(\{T_{21}, T_{11}\}/x) = \mathrm{Zero}(\mathbb{T}_2^{(2)}),\\
\mathcal{Z}_2 &= \mathrm{Zero}(\{T_{31}, T_{11}\}/xT_{21}) = \mathrm{Zero}(\mathbb{T}_3^{(2)}) \cup \mathrm{Zero}(\mathbb{T}_{13}),\\
\mathcal{Z}_3 &= \mathrm{Zero}(\{T_{41}, T_{11}\}/xT_{21}T_{31}) = \mathrm{Zero}(\mathbb{T}_4^{(2)}) \cup \mathrm{Zero}(\mathbb{T}_{12}).
\end{aligned}$$

由此可得

$$\mathrm{Zero}(T_{11}/x) = \mathcal{Z}_1 \cup \mathcal{Z}_2 \cup \mathcal{Z}_3 \cup \mathrm{Zero}(T_{11}/\mathbb{U}_{11}) = \bigcup_{i=1}^{4} \mathrm{Zero}(\mathbb{T}_i^{(2)}/\mathbb{U}_i^{(2)}).$$

于是

$$\bigcup_{i=1}^{5} \mathrm{Zero}(\mathbb{T}_i^{(2)}/\mathbb{U}_i^{(2)}) = \mathrm{Zero}(T_{11}/x) \cup \mathrm{Zero}(\mathbb{T}_5^{(2)}),$$

因此隐式方程 (9.2.1) 被化简为：

$$\begin{aligned}
E &= 729\,x^8 + 216\,x^7 + 729\,x^6y^2 - 2900\,x^6 - 1458\,x^5y^2 - 2376\,x^5\\
&\quad - 2619\,x^4y^2 + 3870\,x^4 - 1458\,x^3y^4 - 4892\,x^3y^2 + 4072\,x^3\\
&\quad + 729\,x^2y^4 - 297\,x^2y^2 - 1188\,x^2 - 4158\,xy^4 + 5814\,xy^2\\
&\quad - 1656\,x + 427\,y^2 - 1685\,y^4 + 729\,y^6 + 529 = 0,\\
x &\neq 0
\end{aligned} \tag{9.2.2}$$

(这里 $E = T_{11}$) 或

$$x = 0,\quad 729\,y^4 - 956\,y^2 - 529 = 0. \tag{9.2.3}$$

也可以由例 3.1.2 中的正则序列或者通过计算带投影的特征序列导出这些方程. $\mathbb{P}$ 的特征列容易计算，但特征序列的计算则需要很长的时间.

可以检验，(9.2.2) 中的第一个方程 $E = 0$ 在 $x = 0$ 时变为

$$(y^2 - 1)\,(729\,y^4 - 956\,y^2 - 529) = 0.$$

因此 $(0,1)$ 和 $(0,-1)$ 都是 $E=0$ 的解，可是这两点并不在参数曲线上（即不存在相应的 u,v 和 w 使参数方程得以满足）. 这就是为什么在 $x=0$ 的情形我们需要用 (9.2.3) 来代替 (9.2.2). 综合上述，我们有如下结论：

- 参数方程所定义的曲线上的每一点 (x,y) 都在隐式方程 $E=0$ 所定义的曲线上；
- 隐式方程 $E=0$ 所定义的曲线上的任一不同于 $(0,1)$ 和 $(0,-1)$ 的点 (x,y) 也都在参数方程所定义的曲线上.

消去法还能用来处理几个与参数对象隐式化有关的问题，如参数的独立性，参数化的适当性和反演问题.

9.3 奇点的存在性条件与检测

奇点的研究不仅是代数几何中的经典课题，而且对现代几何应用也很重要. 例如，在描绘代数曲线时，我们首先要检测出数值方法难以对付的所有奇点. 在研究机器人的运动行为时，我们必须定出那些奇异构形；因为在奇异状态机器人的手臂难以移动. 本节说明如何建立参数代数超曲面具有任意重奇点的充分必要条件，通过计算不可约分解来刻画奇点簇的结构，并在奇点的个数有限时求出所有奇点.

n 维投影空间 $\mathbf{P}^n$ 或仿射空间 $\mathbf{A}^n$ 中的代数超曲面 $\mathfrak{H}$ 是单个齐次多项式方程 $F(x_0,\boldsymbol{x})=0$ 或“通常的”多项式方程 $F(\boldsymbol{x})=0$ 所定义的 $n-1$ 维代数簇. 在 $n=2,3$ 时，分别称其为*代数曲线*或*代数曲面*. $\mathbf{P}^n$ 中 $\mathfrak{H}$ 上一点 $(\bar{x}_0,\bar{\boldsymbol{x}})$ 称为是 p *重*的，如果 F 的所有阶数 $<p$ 的偏导数在 $(\bar{x}_0,\bar{\boldsymbol{x}})$ 处都为零，但某个 p 阶偏导数在 $(\bar{x}_0,\bar{\boldsymbol{x}})$ 处不为零，即

$$\begin{aligned}
&\frac{\partial^r F}{\partial x_0^{r_0}\partial x_1^{r_1}\cdots\partial x_n^{r_n}}(\bar{x}_0,\bar{\boldsymbol{x}})=0 \quad \text{对所有 } r_0+r_1+\cdots+r_n=r<p,\\
&\frac{\partial^r F}{\partial x_0^{r_0}\partial x_1^{r_1}\cdots\partial x_n^{r_n}}(\bar{x}_0,\bar{\boldsymbol{x}})\neq 0 \quad \text{对某一 } r_0+r_1+\cdots+r_n=r=p.
\end{aligned}$$

$\mathbf{A}^n$ 中 $\mathfrak{H}$ 上一点 $\bar{\boldsymbol{x}}$ 称为是 p *重*的，如果

$$\begin{aligned}
&\frac{\partial^r F}{\partial x_1^{r_1}\cdots\partial x_n^{r_n}}(\bar{\boldsymbol{x}})=0 \quad \text{对所有 } r_1+\cdots+r_n=r<p,\\
&\frac{\partial^r F}{\partial x_1^{r_1}\cdots\partial x_n^{r_n}}(\bar{\boldsymbol{x}})\neq 0 \quad \text{对某一 } r_1+\cdots+r_n=r=p
\end{aligned}$$

成立. 任意重数 $p \geq 2$ 的点都称为 $\mathfrak{H}$ 的 奇点.

算法 SinConP: $\Psi \leftarrow \text{SinConP}(F, p)$. 给定 $\mathbf{P}^n$ 中代数超曲面 $\mathfrak{H}$ 的齐次多项式方程 $F(x_0, \boldsymbol{x}) = 0$ 以及整数 $p \geq 1$, 这里 $F \in \mathcal{K}[\boldsymbol{t}, x_0, \boldsymbol{x}]$ 而 $\boldsymbol{t} = (t_1, \cdots, t_m)$ 视为参数, 本算法计算 $n+1$ 个多项式组 $\mathbb{P}_0, \cdots, \mathbb{P}_n \subset \mathcal{K}[\boldsymbol{t}]$ 构成的集合 Ψ, 使得 $\mathfrak{H}$ 对 $\boldsymbol{t} = \bar{\boldsymbol{t}} \in \tilde{\mathcal{K}}^m$ 有重数 $\geq p+1$ 的奇点当且仅当

$$\bar{\boldsymbol{t}} \in \bigcup_{i=0}^{n} \text{Zero}(\mathbb{P}_i).$$

S1. 命

$$\mathbb{D} \leftarrow \left\{ \frac{\partial^p F}{\partial x_0^{r_0} \partial x_1^{r_1} \cdots \partial x_n^{r_n}} : \ r_0 + r_1 + \cdots + r_n = p \right\}.$$

对 $0 \leq i \leq n$ 计算 $\mathbb{D}|_{x_i=1}$ 关于 $t_1 \prec \cdots \prec t_m \prec x_0 \prec \cdots \prec x_n$ 的纯字典项序格罗布讷基 $\mathbb{G}_i$.

S2. 对 $0 \leq i \leq n$ 置 $\mathbb{P}_i \leftarrow \mathbb{G}_i \cap \mathcal{K}[\boldsymbol{t}]$, 且命 $\Psi \leftarrow \{\mathbb{P}_0, \cdots, \mathbb{P}_n\}$.

证　假设 $\mathfrak{H}$ 对某一 $\boldsymbol{t} = \bar{\boldsymbol{t}}$ 有重数 $\geq p+1$ 的奇点 $\bar{\boldsymbol{x}}$; 则 $(\bar{\boldsymbol{t}}, \bar{\boldsymbol{x}}) \in \text{Zero}(\mathbb{D})$. 因平凡零点 $\mathbf{0}$ 不计算在内, 故存在 i, $0 \leq i \leq n$, 使得 $\bar{x}_i \neq 0$. 由此可见

$$\left(\bar{\boldsymbol{t}}, \frac{\bar{x}_0}{\bar{x}_i}, \cdots, \frac{\bar{x}_{i-1}}{\bar{x}_i}, 1, \frac{\bar{x}_{i+1}}{\bar{x}_i}, \cdots, \frac{\bar{x}_n}{\bar{x}_i}\right) \in \text{Zero}(\mathbb{D}|_{x_i=1}) = \text{Zero}(\mathbb{G}_i).$$

所以

$$\bar{\boldsymbol{t}} \in \text{Zero}(\mathbb{G}_i \cap \mathcal{K}[\boldsymbol{t}]) = \text{Zero}(\mathbb{P}_i). \tag{9.3.1}$$

另一方面, 设 (9.3.1) 对某个 i 成立, $0 \leq i \leq n$; 不失一般性, 假定 $i = 0$, 那么

$$\bar{\boldsymbol{t}} \in \text{Zero}(\text{Ideal}(\mathbb{G}_0) \cap \mathcal{K}[\boldsymbol{t}]) = \text{Zero}(\text{Ideal}(\mathbb{D}|_{x_0=1}) \cap \mathcal{K}[\boldsymbol{t}]).$$

设 $\mathbb{R}$ 为 $\mathbb{D}$ 关于 $x_0, \boldsymbol{x}$ 的结式系统. 由引理 1.3.1 和 5.4 节中 $\mathbb{R}$ 的构造可知, 对任意 $R \in \mathbb{R}$ 都存在整数 k, 使得 $Rx_0^k \in \text{Ideal}(\mathbb{D})$. 这也可以从 (5.4.4) 式和 [71] (第 8 页) 看出. 于是

$$\text{Zero}(\text{Ideal}(\mathbb{D}|_{x_0=1}) \cap \mathcal{K}[\boldsymbol{t}]) \subset \text{Zero}(R), \quad \forall R \in \mathbb{R}.$$

因此对所有 $R \in \mathbb{R}$ 都有 $R(\bar{\boldsymbol{t}}) = 0$. 依定理 5.4.3, $\mathbb{D}|_{\boldsymbol{t}=\bar{\boldsymbol{t}}}$ 关于 $\boldsymbol{x}$ 在 $\mathcal{K}(\bar{\boldsymbol{t}})$ 的某一扩域中有非平凡零点 $\bar{\boldsymbol{x}}$. 换言之, $\mathfrak{H}$ 对 $\boldsymbol{t} = \bar{\boldsymbol{t}}$ 有重数 $\geq p+1$ 的奇点 $\bar{\boldsymbol{x}}$. 如所欲证. □

现在考虑仿射空间 $\mathbf{A}^n$ 中的超曲面. 设 F 为 $\mathcal{K}[\boldsymbol{x}]$ 中全次数为 m 的多项式, 而 F_i 是 F 的全次数为 i 的齐次部分, $0 \le i \le m$. 我们定义

$$\frac{\partial F}{\partial 1} \triangleq F_{m-1} + 2\,F_{m-2} + \cdots + mF_0$$

以及相应的 F 对 1 的高阶导数. 容易验证如下欧拉关系:

$$\frac{\partial F}{\partial 1} = mF - \sum_{i=1}^{n} x_i \frac{\partial F}{\partial x_i}.$$

算法 SinConA: $\Psi \leftarrow \mathrm{SinConA}(F, p)$. 给定 $\mathbf{A}^n$ 中代数超曲面 $\mathfrak{H}$ 的多项式方程 $F(\boldsymbol{x}) = 0$ 和整数 $p \ge 1$, 这里 $F \in \mathcal{K}[\boldsymbol{t}, \boldsymbol{x}]$ 而 $\boldsymbol{t} = (t_1, \cdots, t_m)$ 视为参数, 本算法计算有限多个 $\mathcal{K}[\boldsymbol{t}]$ 中多项式系统 $[\mathbb{P}_1, \mathbb{Q}_1], \cdots, [\mathbb{P}_e, \mathbb{Q}_e]$ 组成的集合 Ψ, 使得 $\mathfrak{H}$ 对 $\boldsymbol{t} = \bar{\boldsymbol{t}} \in \tilde{\mathcal{K}}^m$ 有重数 $\ge p + 1$ 的奇点当且仅当

$$\bar{\boldsymbol{t}} \in \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{P}_i / \mathbb{Q}_i).$$

S1. 命

$$\mathbb{D} \leftarrow \left\{ \frac{\partial^p F}{\partial 1^{r_0} \partial x_1^{r_1} \cdots \partial x_n^{r_n}} :\ r_0 + r_1 + \cdots + r_n = p \right\}.$$

计算 $\mathbb{D}$ 关于变元序 $t_1 \prec \cdots \prec t_m \prec x_1 \prec \cdots \prec x_n$ 对 $\boldsymbol{x}$ 带投影的三角序列 Ψ. 若 $\Psi = \emptyset$, 则 $\mathfrak{H}$ 对任意 $\boldsymbol{t}$ 都无奇点; 这时算法终止.

S2. 从 $\bigcup_{[\mathbb{T},\mathbb{U}] \in \Psi} \mathrm{Zero}(\mathbb{T} \cap \mathcal{K}[\boldsymbol{t}] / \mathbb{U} \cap \mathcal{K}[\boldsymbol{t}])$ 中抹去多余的集合, 将其化简, 并设所得的零点集为 $\bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{P}_i / \mathbb{Q}_i)$. 输出

$$\Psi \leftarrow \{[\mathbb{P}_1, \mathbb{Q}_1], \cdots, [\mathbb{P}_e, \mathbb{Q}_e]\}.$$

证 由三角序列的定义和 $[\mathbb{T}, \mathbb{U}] \in \Psi$ 的投影性质即得. □

注 9.3.1 加上投影, 三角序列也可以用来确定投影超曲面存在奇点的条件; 同样, 格罗布讷基可以用来确定仿射超曲面有奇点的条件.

在超曲面 $\mathfrak{H}$ 对特定化的 $\boldsymbol{t}$ 有重数 $\ge p+1$ 的奇点时, 奇点 (代数) 簇的结构可以通过计算其不可约分解予以描述; 每个分支的维数从不可约分解立即可得. 在奇点的个数有限时, 计算所有奇点等于解三角化的多项式方程和不等方程组.

在超曲面有重数 $\ge p + 1$ 的奇点之条件以及奇点簇的结构确定之后, 我们便容易确定 $\mathfrak{H}$ 有 $p + 1$ 重奇点的充要条件以及相应奇点簇对特定化的 $\boldsymbol{t}$ 的结构: 只需简单地引进不等方程.

例 9.3.1 考虑 $\mathbf{P}^3$ 中由方程

$$F = x_0^3 + x_1^3 + x_2^3 + x_3^3 + 3\,ax_0x_1x_2 + 3\,bx_1x_2x_3 = 0$$

定义的投影代数曲面. F 的四个一阶偏导数在除去常数 3 之后构成集合

$$\mathbb{D} = \{ax_1x_2 + x_0^2, bx_2x_3 + ax_0x_2 + x_1^2, bx_1x_3 + ax_0x_1 + x_2^2, x_3^2 + bx_1x_2\}.$$

对 $0 \leq i \leq 3$ 计算 $\mathbb{D}|_{x_i=1}$ 的格罗布讷基, 我们发现四个格罗布讷基中有且仅有一个只含变元 a 和 b 的多项式

$$\delta = a^6 - 2\,a^3b^3 + b^6 + 2\,a^3 + 2\,b^3 + 1.$$

所以投影曲面有奇点当且仅当 $\delta = 0$. 使用同一方法我们可以发现该曲面没有重数 ≥ 3 的奇点.

现考虑用 1 替换 x_0 之后的特殊情形:

$$\bar{F} = F|_{x_0=1} = 1 + x_1^3 + x_2^3 + x_3^3 + 3\,ax_1x_2 + 3\,bx_1x_2x_3 = 0$$

在三维仿射空间中定义一代数曲面. 关于序 $a \prec b \prec x_1 \prec x_2 \prec x_3$,

$$\mathbb{D}_0 = \left\{\frac{\partial \bar{F}}{\partial 1}, \frac{\partial \bar{F}}{\partial x_1}, \frac{\partial \bar{F}}{\partial x_2}, \frac{\partial \bar{F}}{\partial x_3}\right\}$$

的特征序列由以下两个升列组成:

$$\begin{aligned}\mathbb{C}_1 &= [\delta, 2\,a^3x_1^3 + b^3 - a^3 + 1, ax_1x_2 + 1, 2\,a^2bx_3 + b^3 + a^3 + 1],\\ \mathbb{C}_2 &= [a^3 + 1, b, x_1^3 - 1, ax_1x_2 + 1, x_3^2].\end{aligned}$$

对 $i = 1, 2$ 将 $\mathrm{Zero}(\mathbb{C}_i/\mathrm{ini}(\mathbb{C}_i))$ 投影到 a, b, 我们有

$$\begin{aligned}\mathrm{Proj}_{a,b}\mathrm{Zero}(\mathbb{D}_0) &= \mathrm{Proj}_{a,b}\mathrm{Zero}(\mathbb{C}_1/abx_1) \cup \mathrm{Proj}_{a,b}\mathrm{Zero}(\mathbb{C}_2/ax_1)\\ &= \mathrm{Zero}(\delta/ab(a^3 - b^3 - 1)) \cup \mathrm{Zero}(\{a^3 + 1, b\}/a)\\ &= \mathrm{Zero}(\delta/a).\end{aligned}$$

因此曲面 $\bar{F} = 0$ 有奇点当且仅当 $\delta = 0$ 而 $a \neq 0$. 使用同一方法可以发现该曲面无重数 ≥ 3 的奇点.

譬如选取 $a = b = -1/\sqrt[3]{4}$, 它满足每种情形所得的条件. 此时曲面必定有奇点. 为求出所有奇点, 我们简单地将 a, b 的值代入上面的特征序列或格罗

布讷基. 由此容易求得三个奇点如下:

$$(1, \sqrt[3]{2}, \sqrt[3]{2}, 1),$$
$$\left(1, -\frac{\sqrt[3]{2}(\sqrt{3}i+1)}{2}, \frac{\sqrt[3]{2}(\sqrt{3}i-1)}{2}, 1\right),$$
$$\left(1, \frac{\sqrt[3]{2}(\sqrt{3}i-1)}{2}, -\frac{\sqrt[3]{2}(\sqrt{3}i+1)}{2}, 1\right).$$

若取 $a=1$, 则 b 有四个值使得 $\delta=0$. 对其中每个值, 所讨论的曲面有三个奇点. 所有这些奇点都已在例 7.2.1 中求出.

例 9.3.2 对以未定元 $x_1,\cdots,x_4$ 为系数的一元四次方程

$$F = x^4 + x_1x^3 + x_2x^2 + x_3x + x_4 = 0, \tag{9.3.2}$$

我们已在例 5.4.1 中计算了 F 的判别式 Δ_F. 它是一个全次数为 6 的多项式. $\Delta_F=0$ 在四维仿射空间中定义一代数超曲面, 称为 F 的 *判别式曲面*. 让我们来研究该曲面的奇点, 它们的存在性如 $(0,\cdots,0)$ 是显然的. 对于 Δ_F 的四个一阶偏导数构成的多项式组, 其不可约特征序列由以下三个升列组成:

$$\begin{aligned}
\mathbb{C}_1 &= [8\,x_2 - 3\,x_1^2, 16\,x_3 - x_1^3, 256\,x_4 - x_1^4],\\
\mathbb{C}_2 &= [8\,x_3 - 4\,x_1x_2 + x_1^3, 64\,x_4 - 16\,x_2^2 + 8\,x_1^2x_2 - x_1^4],\\
\mathbb{C}_3 &= [108\,x_3^2 - 108\,x_1x_2x_3 + 27\,x_1^3x_3 + 32\,x_2^3 - 9\,x_1^2x_2^2,\\
&\quad 12\,x_4 - 3\,x_1x_3 + x_2^2].
\end{aligned}$$

它们的维数分别是 1,2,2. 由于 $\mathbb{C}_1,\mathbb{C}_2,\mathbb{C}_3$ 中所有多项式的初式都是常数, 每个升列本身就定义了一个不可约代数簇. 于是我们也获得了判别式曲面奇点簇的不可约分解. 检查发现

- $\mathbb{C}_1 = 0 \iff$ (9.3.2) 有一个四重根;
- $\mathbb{C}_2 = 0 \iff$ (9.3.2) 有两个二重根;
- $\mathbb{C}_3 = 0 \iff$ (9.3.2) 有一个三重根.

判别式曲面上剩下的点对应于 (9.3.2) 仅有一个二重根的情形. 这些事实也能通过消去法予以确认: 例如, 收集 $F-(x^2-ax-b)^2$ 关于 x 的系数给出四个 x_i 和 a,b 的多项式组成的集合 $\mathbb{P}$. 计算 $\mathbb{P}$ 关于 $x_1 \prec \cdots \prec x_4 \prec a \prec b$ 的特征列或特征序列即可得出 $\mathbb{C}_2$.

此外，我们也可以考察 Δ_F 的二阶偏导数，它们对 $\mathbb{C}_1$ 的伪余式都为 0，但对 $\mathbb{C}_2$ 和 $\mathbb{C}_3$ 并非如此. 所以 $\mathbb{C}_1$ 的零点，且事实上只有这些零点，是判别式曲面重数 ≥ 3 的奇点. 原点 $(0,\cdots,0)$ 是仅有的重数 >3 的奇点 —— 它的重数为 6. 也容易验证 $\mathrm{Zero}(\mathbb{C}_1)\subset\mathrm{Zero}(\mathbb{C}_i)$, $i=2,3$; 实际上,

$$\mathrm{Zero}(\mathbb{C}_1)=\mathrm{Zero}(\mathbb{C}_2)\cap\mathrm{Zero}(\mathbb{C}_3).$$

所以 $\mathrm{Zero}(\mathbb{C}_1)$ 是可以从分解中抹去的多余分支.

顺便指出，如果所考虑的是五次而非四次多项式，那么涉及的计算要复杂得多. 我们试图研究这一情形而未能获得成功.

9.4 代数因子分解

第一方法

设 $u_1,\cdots,u_d$ 为 d 个超越元，缩写为 $\boldsymbol{u}$, 而 $\mathcal{K}_0=\mathrm{Q}(u_1,\cdots,u_d)$ 是从 Q 通过添加 $u_1,\cdots,u_d$ 所得的扩域. 对任意 $1\leq i\leq r$, $\mathcal{K}_i=\mathcal{K}_0(\eta_1,\cdots,\eta_i)$ 表示从 $\mathcal{K}_0$ 通过依次添加代数元 $\eta_1,\cdots,\eta_i$ 所得的代数扩域，这里 η_i 的添加多项式为 $A_i\in\mathcal{K}_{i-1}[y_i]$. 与往常一样，让 $\boldsymbol{y}_i$ 代表 $y_1,\cdots,y_i$, 而 $\boldsymbol{y}=\boldsymbol{y}_r$. 在多项式 A_i 明确给出时，我们将 $\mathcal{K}_i$ 简写为 $\mathcal{K}_0(\boldsymbol{y}_i)$ 而不再引进 η_i. 不失一般性，假定 $A_i\in\mathcal{K}_0[\boldsymbol{y}_i]$, 那么 $\mathbb{A}=[A_1,\cdots,A_r]$ 构成扩域 $\mathcal{K}_r$ 关于 $\boldsymbol{y}$ 的不可约添加升列 (见 1.4 节).

现将代数因子分解的第一种方法描述如下.

算法 FactorA: $F^*\leftarrow\mathrm{FactorA}(F,\mathbb{A})$. 给定不可约升列 $\mathbb{A}=[A_1,\cdots,A_r]\subset\mathcal{K}_0[\boldsymbol{y}]$ 和次数 $m\geq 1$ 的多项式 $F\in\mathcal{K}_0[\boldsymbol{y},y]$, 该多项式在 $\mathcal{K}_0$ 上不可约且对 $\mathbb{A}$ 是约化的，本算法将 F 在 $\mathcal{K}_r$ 上分解为不可约因子的乘积 F^*, 这里 $\mathcal{K}_r=\mathcal{K}_0(\boldsymbol{y})$ 关于 $\boldsymbol{y}$ 的添加升列为 $\mathbb{A}$.

F1. 若 $m=1$, 则转至 F3. 若 m 为偶数，则命 $\bar{m}\leftarrow m/2$; 否则命 $\bar{m}\leftarrow(m-1)/2$.

F2. 对 $s=1,\cdots,\bar{m}$ 执行下列步骤:

F2.1. 对 $1\leq i\leq r$ 置 $d_i\leftarrow\mathrm{ldeg}(A_i)$, 且命 $t\leftarrow m-s$. 又命

$$G\leftarrow y^s+g_1y^{s-1}+\cdots+g_s,\quad H\leftarrow y^t+h_1y^{t-1}+\cdots+h_t,$$

这里

$$g_i \leftarrow \sum_{\substack{0\le k_l\le d_l-1\\ 1\le l\le r}} g_{ik_1\cdots k_r} y_1^{k_1}\cdots y_r^{k_r}, \qquad 1\le i\le s,$$
$$h_j \leftarrow \sum_{\substack{0\le k_l\le d_l-1\\ 1\le l\le r}} h_{jk_1\cdots k_r} y_1^{k_1}\cdots y_r^{k_r}, \qquad 1\le j\le t,$$

而 $g_{ik_1\cdots k_r}, h_{jk_1\cdots k_r}$ 为新未定元. 设 $g_{ik_1\cdots k_r}$ 和 $h_{jk_1\cdots k_r}$ 的总个数为 M [这时 $M=(s+t)d_1\cdots d_r$], 并将这些未定元重新命名为 $x_1,\cdots,x_M$.

F2.2. 展开 $R\leftarrow F-\mathrm{lc}(F,y)\cdot G\cdot H$, 计算 $R\leftarrow \mathrm{prem}(R,\mathbb{A})$, 并让 R 关于 $\boldsymbol{y}$ 和 y 所有项的系数为 0. 设所得的 $\mathcal{K}_0[x_1,\cdots,x_M]$ 中 M 个多项式方程为

$$\begin{cases} P_1(x_1,\cdots,x_M)=0,\\ P_2(x_1,\cdots,x_M)=0,\\ \quad\cdots\cdots\cdots\cdots\\ P_M(x_1,\cdots,x_M)=0. \end{cases} \tag{9.4.1}$$

F2.3. 用第七章中介绍的方法对 $x_1,\cdots,x_M$ 在 $\mathcal{K}_0$ 中解方程组 (9.4.1). 如果 (9.4.1) 在 $\mathcal{K}_0$ 中无解, 则回到 F2 执行下一个 s. 否则, 设 $x_1=\bar{x}_1,\cdots,x_M=\bar{x}_M$ 为 (9.4.1) 的任意一组解, 命

$$G\leftarrow G|_{x_1=\bar{x}_1,\cdots,x_M=\bar{x}_M}, \quad H\leftarrow H|_{x_1=\bar{x}_1,\cdots,x_M=\bar{x}_M},$$

并转至 F4 [此时 F 在 $\mathcal{K}_r$ 上的分解为 $F\doteq \mathrm{lc}(F,y)\cdot G\cdot H$].

F3. 输出 $F^*\leftarrow F$ [这时 F 在 $\mathcal{K}_r$ 上不可约], 且算法终止.

F4. 在 $\mathcal{K}_r$ 上分解 G 和 H, 并输出

$$F^*\leftarrow \mathrm{lc}(F,y)\cdot \mathrm{FactorA}(G,\mathbb{A})\cdot \mathrm{FactorA}(H,\mathbb{A}).$$

证 显然. □

在上述算法中, 代数因子分解被化为多项式方程求解. 换言之, F 能否在 $\mathcal{K}_r$ 上分解为因子 G 和 H 之积等价于 (9.4.1) 对 $x_1,\cdots,x_M$ 在 $\mathcal{K}_0$ 中是否有解. 胡森和笔者在 [32] 中说明了如何用特征列方法以及高斯引理来判定 (9.4.1) 的可解性和求其在 $\mathcal{K}_0$ 中的解.

例 9.4.1 考虑下列多项式:

$$\begin{aligned}H_1 &= u_3y_1^2 + 2\,u_1u_2y_1 + 2\,u_1^2y_1 - u_1^2u_3,\\ H_2 &= u_3y_2^2 - 2\,u_1u_2y_2 + 2\,u_1^2y_2 - u_1^2u_3,\\ H_3 &= u_3y_3^2 - u_3^2y_3 - u_2^2y_3 + u_1^2y_3 - u_1^2u_3\end{aligned}$$

(见例 9.4.3). 令 $\mathcal{K}_0 = \mathbb{Q}(u_1, u_2, u_3)$. 我们首先验证 H_2 在 $\mathcal{K}_1 = \mathcal{K}_0(y_1)$ 上的不可约性, 这里 y_1 是以 H_1 为添加多项式的代数元. 为此, 命

$$G = y_2 + g_1y_1 + g_0,\quad H = y_2 + h_1y_1 + h_0,$$

则

$$R = \mathrm{prem}\,(H_2 - \mathrm{lc}(H_2, y_2)\cdot G\cdot H, H_1, y_1) = R_1y_1y_2 + R_2y_2 + R_3y_1 + R_4,$$

其中

$$\begin{aligned}R_1 &= u_3\,(g_1 + h_1),\\ R_2 &= u_3\,(g_0 + h_0) + 2\,u_1\,(u_2 - u_1),\\ R_3 &= -2\,u_1\,(u_2 + u_1)\,g_1h_1 + u_3\,(g_1h_0 + g_0h_1),\\ R_4 &= u_3\,(u_1^2g_1h_1 + g_0h_0 + u_1^2).\end{aligned}$$

置 $\mathbb{P} = \{R_1, \cdots, R_4\}$. 为了确定 $\mathbb{P} = 0$ 对 g_1, g_0 和 h_1, h_0 在 $\mathcal{K}_0$ 中是否有解, 我们计算 $\mathbb{P}$ 在 $g_0 \prec h_0 \prec h_1 \prec g_1$ 之下的特征序列. 该序列由以下两个拟线性升列组成:

$$\mathbb{C}_1 = \begin{bmatrix} u_3\,(u_3^2 + \mu^2)\,g_0^2 + 2\,u_1\nu\,(u_3^2 + \mu^2)\,g_0 - 4\,u_1^3u_2u_3,\\ u_3h_0 + u_3g_0 + 2\,u_1\nu,\\ u_1\mu h_1 + u_3g_0 + u_1\nu,\\ u_1\mu g_1 - u_3g_0 - u_1\nu \end{bmatrix},$$

$$\mathbb{C}_2 = [u_3g_0^2 + 2\,u_1\nu g_0 - u_1^2u_3, u_3h_0 + u_3g_0 + 2\,u_1\nu, h_1, g_1],$$

其中

$$\mu = u_2 + u_1,\quad \nu = u_2 - u_1.$$

$\mathbb{C}_1$ 和 $\mathbb{C}_2$ 中的第一个多项式在 $\mathbb{Q}$ 上都不可约, 因此系统 $\mathbb{C}_1 = 0 \wedge \mathrm{ini}(\mathbb{C}_1) \neq 0$ 和 $\mathbb{C}_2 = 0 \wedge \mathrm{ini}(\mathbb{C}_2) \neq 0$ 在 $\mathcal{K}_0$ 中都无解. 所以, 多项式 H_2 在 $\mathcal{K}_1$ 上是不可约的.

现在我们要在 $\mathcal{K}_2 = \mathcal{K}_1(y_2)$ 上分解 H_3, 此时 H_2 是 y_2 的添加多项式. 遵照算法步骤, 命

$$G = y_3 + g_{11}y_1y_2 + g_{01}y_2 + g_{10}y_1 + g_{00},$$
$$H = y_3 + h_{11}y_1y_2 + h_{01}y_2 + h_{10}y_1 + h_{00}.$$

多项式

$$R = \operatorname{prem}(H_3 - \operatorname{ini}(H_3) \cdot G \cdot H, [H_1, H_2])$$

有 46 项, 这里 $y_1 \prec y_2 \prec y_3$. 令 R 关于 y_1, y_2, y_3 的系数为 0, 我们得到例 7.2.3 中给出的多项式方程组 (7.2.2). 该例中已求得 (7.2.2) 关于 h_{ij} 和 g_{ij} 的一组解, 如 (7.2.3) 所示. 于是 H_3 的因子分解为

$$H_3 \doteq \frac{(2\,u_1^2y_3 - F - u_1^2u_3)\cdot[2\,u_1^2u_3y_3 + u_3F - u_1^2\,(u_3^2 + 2\,u_2^2 - 2\,u_1^2)]}{4\,u_1^4}, \tag{9.4.2}$$

其中

$$F = u_3y_1y_2 + u_1\,(u_2 + u_1)\,y_2 - u_1\,(u_2 - u_1)\,y_1.$$

第二方法

这一方法的关键想法是通过线性变换和特征列计算将代数扩域上的多项式因子分解化为 Q 上的因子分解. 设 $\mathbb{A} = [A_1, \cdots, A_r]$, $\mathcal{K}_i$ 和 F 与 FactorA 中相同. 置

$$\mathbb{A}^+ = [A_1, \cdots, A_r, F].$$

关于 $y_1 \prec \cdots \prec y_r \prec y$, $\mathbb{A}^+$ 明显为一升列, 并且 F 在 $\mathcal{K}_r$ 上不可约当且仅当 $\mathbb{A}^+$ 不可约. 在说到 G 是 F 在 $\mathcal{K}_r$ 上的因子时, 我们总是指 $\deg(G, y) > 0$ (即 G 不是 $\mathcal{K}_r$ 中的数). 如果 $0 < \deg(G, y) < \deg(F, y)$, 则称 G 为 F 的*真因子*.

假定我们已知如何在 $\mathcal{K}_0$ 上将多项式分解为不可约因子. 接下来的引理保证了下述代数因子分解算法的正确性.

引理 9.4.1 设 $\mathbb{A}$ 和 F 同上, $c_1, \cdots, c_r$ 为 r 个整数,

$$\bar{F} = F|_{y = y - c_1y_1 - \cdots - c_ry_r},$$

而 $\bar{\mathbb{C}}$ 是 $\bar{\mathbb{A}} = \mathbb{A} \cup [\bar{F}]$ 在 $\mathcal{K}_0$ 上关于序 $y \prec y_1 \prec \cdots \prec y_r$ 的特征序列中任一升列. 又设 $\bar{C}$ 为 $\bar{\mathbb{C}}$ 中的第一个多项式, 而

$$C = \bar{C}|_{y = y + c_1y_1 + \cdots + c_ry_r}.$$

如果 $\bar{\mathbb{C}}$ 是完美的，则 $|\bar{\mathbb{C}}| = r+1$. 如果 $\mathbb{C}$ 是不可约的，则在 $\mathcal{K}_r$ 上 F 和 C 的最大公因子也是不可约的.

证　因 $\mathbb{A}$ 不可约而 F 对 $\mathbb{A}$ 约化，故

$$\mathrm{Dim}(\bar{\mathbb{A}}) = \mathrm{Dim}(\mathbb{A} \cup [F]) = 0.$$

若 $\bar{\mathbb{C}}$ 完美，则 $\dim(\bar{\mathbb{C}}) = 0$. 因此 $|\bar{\mathbb{C}}| = r+1$.

今设 $\bar{\mathbb{C}}$ 不可约，而 $(\eta, \boldsymbol{\eta}) = (\eta, \eta_1, \cdots, \eta_r)$ 为 $\bar{\mathbb{C}}$ 的一般零点，则 $(\eta, \boldsymbol{\eta}) \in \mathrm{Zero}(\bar{\mathbb{A}})$. 于是 $\bar{F}$ 在 $\mathcal{K}_r$ 上有不可约因子 $\bar{G}$, 使得 $\bar{G}(\eta, \boldsymbol{\eta}) = 0$; $(\eta, \boldsymbol{\eta})$ 为 $\mathbb{A} \cup [\bar{G}]$ 的一般零点. 依引理 4.5.1, $\mathrm{prem}(\bar{C}, \mathbb{A} \cup [\bar{G}]) = 0$. 由此可见，在 $\mathcal{K}_r$ 上 $G = \bar{G}|_{y=y+c_1y_1+\cdots+c_ry_r}$ 是 C 的因子.

设 $\bar{H}$ 为 $\bar{F}$ 在 $\mathcal{K}_r$ 上另一个与 $\bar{G}$ 不同 的不可约因子，那么在 $\mathcal{K}_r$ 的某一扩域中存在 η', 使得

$$\bar{H}(\eta', \boldsymbol{\eta}) = 0, \quad \bar{G}(\eta', \boldsymbol{\eta}) \neq 0, \quad \forall \boldsymbol{\eta} \in \mathrm{Zero}(\mathbb{A}).$$

我们断言 $\mathrm{prem}(\bar{C}, \mathbb{A} \cup [\bar{H}]) \neq 0$; 因为否则有 $C(\eta') = 0$, 并能求出 $\boldsymbol{\eta}'$, 使得 $(\eta', \boldsymbol{\eta}') \in \mathrm{Zero}(\bar{\mathbb{C}}) \subset \mathrm{Zero}(\mathbb{A} \cup [\bar{G}])$. 这将引起矛盾. 所以 $\bar{H}$ 不能是 $\bar{C}$ 在 $\mathcal{K}_r$ 上的因子.

设 $\bar{C}$ 在 $\mathcal{K}_r$ 上分解为 $\bar{C} \doteq \bar{D}\bar{G}$, 那么 $\bar{C} - \bar{D}\bar{G} \in \mathrm{sat}(\mathbb{A})$. 剩下的是要证明在 $\mathcal{K}_r$ 上 $\bar{G}$ 不是 $\bar{D}$ 的因子.

因 $\mathrm{prem}(\bar{G}, \mathbb{A}) \neq 0$, 故由引理 3.2.5 和 4.5.2 知存在多项式 $Q \in \mathcal{K}_0[y, \boldsymbol{y}]$, 使得

$$Q\bar{G} - R \in \mathrm{Ideal}(\mathbb{A}) \subset \mathrm{sat}(\mathbb{A}), \quad \text{这里 } R = \mathrm{res}(\bar{G}, \mathbb{A}) \neq 0, \ R \in \mathcal{K}_0[\boldsymbol{y}],$$

且对任意 $(\eta, \boldsymbol{\eta}) \in \mathrm{Zero}(\mathbb{A} \cup [\bar{G}])$ 有 $Q(\eta, \boldsymbol{\eta}) \neq 0$. 由于 $\bar{\mathbb{C}}$ 的每个零点都是 $\mathbb{A} \cup [\bar{G}]$ 的零点，所以 $\bar{C}$ 的每个零点也是 R 的零点. 因此 $\bar{C} \mid R$, 于是存在 $T \in \mathcal{K}_0[\boldsymbol{y}]$, 使得 $R = T\bar{C}$. 由此可知

$$Q\bar{G} - T\bar{D}\bar{G} \in \mathrm{sat}(\mathbb{A}).$$

又因为 $\mathrm{sat}(\mathbb{A})$ 是素理想而 $\bar{G} \notin \mathrm{sat}(\mathbb{A})$, 故 $Q - T\bar{D} \in \mathrm{sat}(\mathbb{A})$. 因此对任意 $(\eta, \boldsymbol{\eta}) \in \mathrm{Zero}(\mathbb{A} \cup [\bar{G}])$ 有

$$Q(\eta, \boldsymbol{\eta}) - \bar{D}(\eta, \boldsymbol{\eta})T(\eta) = 0.$$

注意 $Q(\eta, \boldsymbol{\eta}) \neq 0$. 如果在 $\mathcal{K}_r$ 上 $\bar{G}$ 是 $\bar{D}$ 的因子，则 $\bar{D}(\eta, \boldsymbol{\eta}) = 0$, 因而导致矛盾. 至此我们就证明了 $\bar{G} \nmid \bar{D}$; 所以 $\bar{G}$ 是 $\bar{F}$ 和 $\bar{C}$ 在 $\mathcal{K}_r$ 上的最大公因子. 引理获证. □

我们沿用上面的符号，并设 $\bar{\mathbb{C}} = [\bar{C}_0, \bar{C}_1, \cdots, \bar{C}_r]$ 为 $\bar{\mathbb{A}}$ 的特征列，而 $\bar{J} = \prod_{i=1}^{r} \mathrm{ini}(\bar{C}_i)$. 假设 $\bar{\mathbb{C}}$ 是完美的，因此 $\bar{C}_0 \in \mathcal{K}_0[y]$. 选取 $\bar{C}_0$ 在 $\mathcal{K}_0$ 上不整除 $\bar{J}$ 的不可约因子 $\bar{C}$ (如果有这样的因子)，并在 $\mathcal{K}_r$ 上计算 F 和 $C = \bar{C}|_{y=y+c_1y_1+\cdots+c_ry_r}$ 的最大公因子 G. 在任何情形，如果 G 是 F 在 $\mathcal{K}_r$ 上的真因子，我们便已有所获. 否则，检查 $\bar{\mathbb{C}}$ 是否拟线性. 若是，则

$$[\bar{C}, \mathrm{prem}(\bar{C}_1, \bar{C}), \cdots, \mathrm{prem}(\bar{C}_r, \bar{C})]$$

为 $\bar{\mathbb{A}}$ 的特征序列中一不可约升列. 于是按照引理 9.4.1, G 是 F 在 $\mathcal{K}_r$ 上的不可约因子. 因此，我们需要的是得到拟线性并且完美的 $\bar{\mathbb{C}}$. 引进带随机整数 c_i 的线性变换 $y \leftarrow y - c_1y_1 - \cdots - c_ry_r$ 正是为了使 $\bar{\mathbb{C}}$ 拟线性.

F 和 C 在 $\mathcal{K}_r$ 上的最大公因子可以从 (或者作为) $\mathbb{A} \cup \{F, C\}$ 的特征列中最后一个多项式得到. 此外，也可以通过在 $\mathcal{K}_r$ 上计算 F 与 $\bar{J}|_{y=y+c_1y_1+\cdots+c_ry_r}$ 之不可约因子的最大公因子来构造 F 的可能真因子. 在 $\mathbb{C}$ 拟线性时，获得真因子的机会较高.

有一个重要的实际问题值得一提：F 在 $\mathcal{K}_r$ 上的因子分解只在相差 $\mathcal{K}_r$ 中 "常数" 因子的意义下是唯一的，而该常数因子在这里表示为 $\boldsymbol{u}$ 和 $\boldsymbol{y}$ 的多项式. 这样的常数可以戏剧性地影响 F 的各个因子的大小. 设 G 为 F 的不可约因子；不失一般性，又假定 $G \in \mathbb{Q}[\boldsymbol{u}, \boldsymbol{y}, y]$. 一般来说，$\mathrm{lc}(G, y)$ 既含有变元 $\boldsymbol{u}$ 又含有变元 $\boldsymbol{y}$. 使用算法 Norm 或 NormG, 我们可以用 $\mathbb{A}$ 将 G 正规化以获得另一多项式 $G^* \in \mathbb{Q}[\boldsymbol{u}, \boldsymbol{y}, y]$, 使得 $\mathrm{lc}(G^*, y) \in \mathbb{Q}[\boldsymbol{u}]$, 且 G^* 与 G 只差一个 $\mathcal{K}_r$ 中的因子. 在很多情形 G^* 都比 G 简单得多，但在很多其他情形 G^* 又会比 G 复杂得多. 启发式地使用这种正规化可以大大提高 FactorB 的效率.

算法 FactorB: $F^* \leftarrow \mathrm{FactorB}(F, \mathbb{A})$. 给定不可约升列 $\mathbb{A} = [A_1, \cdots, A_r] \subset \mathcal{K}_0[\boldsymbol{y}]$ 和多项式 $F \in \mathcal{K}_0[\boldsymbol{y}, y]$, 该多项式在 $\mathcal{K}_0$ 上不可约且对 $\mathbb{A}$ 是约化的，本算法将 F 在 $\mathcal{K}_r$ 上分解为不可约因子的乘积 F^*, 这里 $\mathcal{K}_r = \mathcal{K}_0(\boldsymbol{y})$ 关于 $\boldsymbol{y}$ 的添加升列为 $\mathbb{A}$.

F1. 命 $\mathbb{A}^* \leftarrow [A\colon \mathrm{ldeg}(A) > 1, A \in \mathbb{A}]$. 若 $\mathbb{A}^* = \emptyset$ 或者 $\deg(F, y) \le 1$, 则输出 $F^* \leftarrow F$, 且算法终止. 否则，设 $y_{p_1} \prec \cdots \prec y_{p_s}$ 为 $\mathbb{A}^*$ 中多项式的导元，且命 $\Omega \leftarrow \emptyset$.

F2. 选取一组整数 $[c_1, \cdots, c_s] \notin \Omega$, 且命

$$\Omega \leftarrow \Omega \cup \{[c_1, \cdots, c_s]\}, \quad \bar{F} \leftarrow F|_{y=y-c_1y_{p_1}-\cdots-c_sy_{p_s}}.$$

计算 $\mathbb{A}^* \cup \{\bar{F}\}$ 关于变元序 $y \prec y_{p_1} \prec \cdots \prec y_{p_s}$ 的特征列 $\bar{\mathbb{C}}$. 若 $|\bar{\mathbb{C}}| \ne s+1$, 则回到 F2. 设 $\mathbb{I}$ 为 $\mathrm{ini}(\bar{\mathbb{C}})$ 中多项式 (在 $\mathcal{K}_0$ 上) 的所有不可

约因子构成的集合，而 $\mathbb{F}$ 为 $\bar{\mathbb{C}}$ 中第一个多项式 (在 $\mathcal{K}_0$ 上) 的 —— 那些不整除 $\mathbb{I}$ 中任何多项式的 —— 不可约因子所构成的集合.

F3. 若 $\bar{\mathbb{C}}$ 拟线性，则转至 F4. 若 $|\mathbb{F}| \le 1$, 则转至 F2; 否则，命 $\mathbb{I} \leftarrow \mathbb{I} \cup \mathbb{F}$, 而 $\mathbb{F} \leftarrow \emptyset$.

F4. 命 $G \leftarrow F$, $\mathbb{P} \leftarrow \emptyset$, $\mathbb{P}' \leftarrow \emptyset$, 且

$$\mathbb{F} \leftarrow \mathbb{F}|_{y=y+c_1 y_{p_1}+\cdots+c_s y_{p_s}}, \quad \mathbb{I} \leftarrow \mathbb{I}|_{y=y+c_1 y_{p_1}+\cdots+c_s y_{p_s}}.$$

对每个 $P \in \mathbb{F} \cup \mathbb{I}$ 只要 $\deg(G, y) > 1$ 就执行下列步骤:

计算 G 和 P 在 $\mathcal{K}_r$ 上的最大公因子 F_P, 并启发式地将其正规化. 若 $0 < \deg(F_P, y) < \deg(G, y)$, 则在 $\mathcal{K}_r$ 上命 $G \leftarrow G/F_P$, 并且在 $P \in \mathbb{F}$ 时命 $\mathbb{P} \leftarrow \mathbb{P} \cup \{F_P\}$, 否则命 $\mathbb{P}' \leftarrow \mathbb{P}' \cup \{F_P\}$.

F5. 若 $\mathbb{P} \cup \mathbb{P}' \neq \emptyset$, 则输出

$$F^* \leftarrow \prod_{P \in \mathbb{P}} P \cdot \prod_{P \in \mathbb{P}' \cup \{G\}} \mathrm{FactorB}(P, \mathbb{A}^*),$$

且算法终止. 如果 $\bar{\mathbb{C}}$ 拟线性而且 $\mathbb{F} \neq \emptyset$, 则输出 $F^* \leftarrow F$; 否则，回到 F2.

FactorB 的正确性由引理 9.4.1 即得，但不易看出该算法是否一定终止，即完美拟线性特征列能否总在有限步内产生. 所幸的是，用步骤 F2 中随机选取的整数 $c_1, \cdots, c_s$ 获得拟线性特征列的概率为 1. 这是因为在一般情形

$$\deg(\mathrm{prem}(P, Q, x), x) = \deg(Q, x) - 1,$$

而 prem 是特征列算法中的主要运算. 因此在实际计算时，终止性对我们来说从来就不是问题.

在 FactorB 的步骤 F2 中可改为计算特征序列 (而不只是特征列). F 的不可约因子则从序列中那些不可约性容易验证的升列求得. 变元 $y, y_{p_1}, \cdots, y_{p_s}$ 的序也可以是任意的，只要 y 排得最低即可. 由于这一步的目的是通过逐次消元产生 $\mathcal{K}_0[y]$ 中的多项式，其他消去法也同样适用. 事实上，算法 FactorB 可以看作是基于结式计算的特拉格 [70] 方法的一种变形.

上面介绍的两个算法都足够一般. 如果超越元 $\boldsymbol{u}$ 在添加多项式 A_i 中不出现，那么可将因子分解视为在通常所称的 代数数域 $\mathbb{Q}(\boldsymbol{y})$ 上进行. 如果 $\boldsymbol{u}$ 在 A_i 中出现，因子分解则在 代数函数域 $\mathcal{K}_r$ 上进行. 在这后一情形，算法相对要慢不少，主要是因为 $\boldsymbol{u}$ 的出现大大增加了消元和计算最大公因子的复杂性.

例 9.4.2 在计算例 8.3.3 中的不可约分解时，需要用到好几个多项式在代数扩域上的因子分解. 我们选取其中之一作为示范：将

$$F = 4\,y_5^2 - 4\,u_1y_5 - 4\,y_5 - 3\,u_2^2 + u_1^2 + 2\,u_1 + 1$$

在 $\mathbb{Q}(u_1, u_2, y_2)$ 上分解为不可约因子，这里 y_2 的添加多项式为 $A = 4\,y_2^2 - 3$.

用 $y_5 + y_2$ 替换 F 中的 y_5，我们有

$$\begin{aligned}\bar{F} &= F|_{y_5=y_5+y_2}\\ &= 4\,[y_5^2 + (2\,y_2 - u_1 - 1)\,y_5 + y_2^2 - (u_1+1)\,y_2] - 3\,u_2^2 + u_1^2 + 2\,u_1 + 1.\end{aligned}$$

$\{\bar{F}, A\}$ 关于序 $y_5 \prec y_2$ 的特征列为

$$\mathbb{C} = [C_1, \bar{F} - A],$$

这里 C_1 可在 $\mathbb{Q}$ 上分解因子为 $(C_0 + 6\,u_2)\,(C_0 - 6\,u_2)$，其中

$$C_0 = 4\,y_5^2 - 4\,(u_1+1)\,y_5 - 3\,u_2^2 + u_1^2 + 2\,u_1 - 2.$$

我们考虑 C_1 的第一个因子，并用 $y_5 - y_2$ 替回其中的 y_5. 所得的多项式为

$$D = 4\,[y_5^2 - (2\,y_2 + u_1 + 1)\,y_5 + y_2^2 + (u_1+1)\,y_2] - 3\,u_2^2 + 6\,u_2 + u_1^2 + 2\,u_1 - 2.$$

为了求 D 和 F 在 $\mathbb{Q}(u_1, u_2, y_2)$ 上的最大公因子，我们计算 $\{D, F, A\}$ 关于序 $y_2 \prec y_5$ 的特征列

$$\bar{\mathbb{C}} = [A, 4\,y_2y_5 - 2\,(u_1+1)\,y_2 - 3\,u_2].$$

$\bar{\mathbb{C}}$ 中的第二个多项式，记作 F_1，是 F 在 $\mathbb{Q}(u_1, u_2, y_2)$ 上的真因子. 将该因子从 F 中除去，我们得到另一个因子

$$F_2 = \mathrm{pquo}(F, F_1, y_5) = 4\,y_2y_5 - 2\,(u_1+1)\,y_2 + 3\,u_2.$$

于是 F 在 $\mathbb{Q}(u_1, u_2, y_2)$ 上分解为两个因子的乘积 $F_1F_2/3$.

注 9.4.1 这里提及几个对实施代数因子分解算法有用的启发式策略. 第一个是代数数论中的结果：设 $A \in \mathcal{K}[x]$ 和 $F \in \mathcal{K}[y]$ 分别是关于 x 次数为 m 和关于 y 次数为 l 的不可约多项式. 如果 m 和 l 互素，那么 F 在以 A 为 x 之添加多项式的代数扩域 $\mathcal{K}(x)$ 上总是不可约的.

其次, 设 $A\in\mathcal{K}[x]$ 和 $F\in\mathcal{K}[y]$ 为两个在 $\mathcal{K}$ 上不可约的多项式, 而 $\tilde{A}$ 和 $\tilde{F}$ 是用 z 将 A 和 F 分别对 x 和 y 齐次化所得的多项式. 又命 $\tilde{R}=\mathrm{prem}(\tilde{F},\tilde{A},z)$, 而 $I=\mathrm{lc}(\tilde{A},z)$, 使得 $I^q\tilde{F}=\tilde{Q}\tilde{A}+\tilde{R}$ 对某一整数 $q\geq 0$ 成立, 那么 $R=\tilde{R}|_{z=1}$ 在 $\mathcal{K}$ 上的任一因子分解除以 I^q 之后都是 F 在以 A 为 x 之添加多项式的代数扩域 $\mathcal{K}(x)$ 上的一个 (不一定完全的) 因子分解. 这是显然的, 只需将 $z=1$ 代入伪余公式即知. 在 $\tilde{R}$ 不含有变元 z 的情形, R 可约的可能性较大.

如果 A 和 F 含有超越元, 上面的齐次化则不需要. 为准确起见, 设 $A\in\mathcal{K}[u,x]$ 和 $F\in\mathcal{K}[u,y]$ 为两个不可约多项式, 且 $\deg(F,u)\geq\deg(A,u)>0$. 又命 $R=\mathrm{prem}(F,A,u)$, 而 $I=\mathrm{lc}(A,u)$, 使得 $I^qF=QA+R$ 对某一整数 $q\geq 0$ 成立, 那么 R 在 $\mathcal{K}$ 上的任一因子分解除以 I^q 并用 A 将其各因子中 x 的高次幂约化之后也是 F 在以 u 为超越元、 A 为 x 之添加多项式的扩域 $\mathcal{K}(u,x)$ 上的一个 (不一定完全的) 因子分解.

来自几何定理机器证明的例子

从 8.3 节中的例子可见, 我们在使用 "自然" 代数表述证明几何定理时需要用代数因子分解来处理可约性问题. 特别指出, 运用某些将几何信息考虑在内的巧妙表述大多数可约性情形都能避免. 然而在因子分解程序有效时, 我们则无需用那些表述技巧. 而且此时, 尽管几何命题的代数表述不与其几何语句精确对应因此不是逻辑意义下的定理, 我们也有可能 "找出" 原命题的证明. 这将帮助我们理解由定理的代数形式所反映出来的、几何上的模棱两可. 现在让我们来回顾前一章中的内旁心定理.

例 9.4.3 参见例 8.2.1, 并将 $\triangle ABC$ 三个顶点的坐标选为

$$A(-u_1,0),\quad B(u_1,0),\quad C(u_2,u_3).$$

设角 A,B,C 的三条平分线与 y 轴分别交于

$$A'(0,y_1),\quad B'(0,y_2),\quad C'(0,y_3).$$

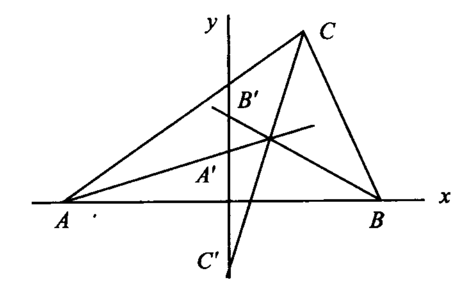


图 16 内旁心定理

那么定理的假设由下列关系组成:

$$\angle CAA' = \angle A'AB, \quad \angle ABB' = \angle B'BC, \quad \angle BCC' = \angle C'CA,$$

而要证的结论为: 三条直线 AA', BB', CC' 共点. 对角的等式取正切, 定理的假设条件对应于三个多项式方程

$$H_1 = 0, \quad H_2 = 0, \quad H_3 = 0;$$

多项式 H_1, H_2, H_3 已在例 9.4.1 中给出. 对变元序 $y_1 \prec y_2 \prec y_3$, 这些多项式已经构成特征列 $\mathbb{C} = [H_1, H_2, H_3]$. 直接验证表明, 结论多项式对 $\mathbb{C}$ 的伪余式不为零. 为了证明定理, 我们需要检查 $\mathbb{C}$ 的可约性. 于是先要检查 H_2 在 $\mathcal{K}_1 = \mathrm{Q}(u_1, u_2, u_3, y_1)$ 上是否可约, 这里 y_1 是以 H_1 为添加多项式的代数元. H_2 在 $\mathcal{K}_1$ 上的不可约性已在例 9.4.1 中得到证实. 下一步是要检查 H_3 在 $\mathcal{K}_2 = \mathcal{K}_1(y_2)$ 上是否可约, 这里 y_2 是以 H_2 为添加多项式的代数元. 在例 9.4.1 中 H_3 已被分解为两个不可约因子之积 (9.4.2). 使用该因子分解, 可以立即将 $\mathbb{C}$ 在 $\mathrm{Q}(u_1, u_2, u_3)$ 上分解为两个不可约分支. 代数形式的定理对其中一个分支成立, 而对另一分支不成立. 这正好与几何事实一致: 从三角形每个角的 (内外) 平分线中各取一条共有八组, 其中四组中的三条分角线共点 (交点分别为三角形的一个内心和三个旁心), 而另外四组中的三条分角线则不共点.

我们将 8.3 节中几何证例所需要的若干代数因子分解罗列如下 (参阅 [82]).

- 设 $\mathrm{Q}(u_1, u_2, y_1)$ 是从 Q 通过添加超越元 u_1, u_2 和以

$$y_1^4 - \alpha y_1^2 + u_1^2$$

为添加多项式的代数元 y_1 所得的扩域, 这里 $\alpha = u_2^2 + u_1^2 + 1$. 在 $\mathrm{Q}(u_1, u_2, y_1)$ 上有下列因子分解:

$$16\, u_2^2 y_9^2 - \alpha^2 + 4\, u_1^2 \doteq (4\, u_2 y_9 + 2\, y_1^2 - \alpha)\, (4\, u_2 y_9 - 2\, y_1^2 + \alpha), \tag{9.4.3}$$

$$\begin{aligned} &16\, u_2^2\, (y_1 + u_1)\, y_{10}^2 - 32\, u_2^2 y_1^3 + 16\, u_1 u_2^2 y_1^2 \\ &+ [u_2^2\, (7\, u_2^2 + 6\, u_1^2 + 22) - (u_1^2 - 1)^2]\, y_1 \\ &- u_1\, [u_2^2\, (u_2^2 + 2\, u_1^2 + 18) + (u_1^2 - 1)^2] \\ &\qquad \doteq \frac{y_1 + u_1}{u_1^2}\, (4\, u_1 u_2 y_{10} + H)\, (4\, u_1 u_2 y_{10} - H), \end{aligned} \tag{9.4.4}$$

其中

$$H = 4\, y_1^3 - 6\, u_1 y_1^2 - 4\, (u_2^2 + 1)\, y_1 + u_1\, (\alpha + 4).$$

- 在计算例 8.3.3 中的 (8.3.2) 时，有几个多项式需要在代数扩域上分解因子. 其中之一的分解

$$4\,y_5^2 - 4\,(u_1+1)\,y_5 - 3\,u_2^2 + 2\,u_1 + u_1^2 + 1 \doteq T_5T_5' \tag{9.4.5}$$

是在扩域 $\mathrm{Q}(u_1,u_2,y_2)$ 上，这里 y_2 的添加多项式为 $4\,y_2^2-3$; 该因子分解的细节已在例 9.4.2 中给出. 下面是同一扩域 $\mathrm{Q}(u_1,u_2,y_2)$ 上的另一因子分解:

$$4\,y_3^2 - 4\,u_1y_3 - 3\,u_2^2 + u_1^2 \doteq T_3T_3'. \tag{9.4.6}$$

- 设 T_3 和 I 与例 8.3.5 中相同，则在 $\mathrm{Q}(u_1,u_2,y_0)$ 上有

$$T_3 \doteq \frac{T_3'T_3''}{I} = \frac{[H+2\,u_1\,(u_2^2+1)\,y_0]\,[H-2\,u_1\,(u_2^2+1)\,y_0]}{I}, \tag{9.4.7}$$

这里 y_0 的添加多项式为 y_0^2-3, 而

$$H = Iy_3 - 2\,u_1\,(3\,u_1u_2^2 + 4\,u_2 - u_1).$$

- 计算例 8.3.6 中的不可约分解时需要用到以 T_1 为 x_1 之添加多项式的扩域 $\mathrm{Q}(u_1,u_2,u_3,x_1)$ 上的下列因子分解:

$$\begin{aligned}&4\,u_2^4\,(2\,u_1^2x_1 - H)\,x_2^2 - 4\,\alpha^2abcdx_2\\&-\alpha^2\,[2\,u_1^2\bar{\alpha}^2x_1 + 2\,u_1^2\gamma u_3 - 4\,(\bar{\gamma}+u_1^2)\,u_2^2u_3 - \bar{\beta}\bar{\alpha}^2]\\&\qquad\doteq \frac{u_2^2\,(2\,u_1^2x_1 - H)}{abcd}\,T_2T_2',\end{aligned} \tag{9.4.8}$$

$$\begin{aligned}&4\,u_2^4\,(2\,u_1^2x_1 + H)\,x_3^2 + 4\,\alpha^2abcdx_3\\&-\alpha^2\,[2\,u_1^2\bar{\alpha}^2x_1 - 2\,u_1^2\gamma u_3 + 4\,(\bar{\gamma}+u_1^2)\,u_2^2u_3 + \bar{\beta}\bar{\alpha}^2]\\&\qquad\doteq \frac{u_2^2\,(2\,u_1^2x_1 + H)}{abcd}\,T_3T_3',\end{aligned} \tag{9.4.9}$$

这里

$$H = 2\,u_1^2u_3 + \bar{\beta};$$

$$\bar{\alpha} = u_2^2 + 1,\quad \bar{\beta} = u_1^4 - 1,\quad \bar{\gamma} = u_1^4 + 1;$$

而 $a,b,c,d,\alpha,\gamma,T_1,T_2,T_2',T_3,T_3'$ 与例 8.3.6 中相同.

- 例 8.3.7 中零点分解的计算需要下列因子分解:

$$2\,x_3^2+2\,x_3-1 \doteq \frac{1}{2}\,(2\,x_3-3\,x_2+1)\,(2\,x_3+3\,x_2+1) \qquad (9.4.10)$$

在以 $3\,x_2^2-1$ 为 (x_2 之) 添加多项式的扩域 $\mathrm{Q}(x_2)$ 上;

$$\begin{aligned} &x_5^2-x_1x_5-x_5+4\,x_1+5\\ &\qquad \doteq \frac{1}{16}\,(4\,x_5-x_1x_2+5\,x_2-2\,x_1-2)\\ &\qquad\qquad \cdot\,(4\,x_5+x_1x_2-5\,x_2-2\,x_1-2) \end{aligned} \qquad (9.4.11)$$

在以

$$[x_1^2-6\,x_1-11,\,x_1x_2^2+3\,x_2^2+52\,x_1+76]$$

为 (x_1 和 x_2 之) 添加升列的扩域 $\mathrm{Q}(x_1,x_2)$ 上.

9.5 一类微分系统的中心条件

问　题

考虑中心焦点型平面自治微分系统

$$\frac{dx}{dt}=y+P(x,y),\quad \frac{dy}{dt}=-x+Q(x,y), \qquad (9.5.1)$$

这里 $P(x,y)$ 和 $Q(x,y)$ 是以未定元 $\boldsymbol{u}=(u_1,\cdots,u_e)$ 为系数、各项关于 x 和 y 的全次数都 >1 的多项式. 如 [76] 中所示, 我们可以计算局部正定的多项式 $L(x,y)\in\mathrm{Q}[\boldsymbol{u},x,y]$ 以及多项式 $v_3,v_5,\cdots,v_{2j+1},\cdots\in\mathrm{Q}[\boldsymbol{u}]$, 使得 $L(x,y)$ 沿着 (9.5.1) 之积分曲线的微分具有如下形式:

$$\frac{dL(x,y)}{dt}=v_3y^4+v_5y^6+\cdots+v_{2j+1}y^{2j+2}+\cdots.$$

我们称 v_{2j+1} 为 (9.5.1) 的第 j 个 *李雅普诺夫常数*.

原点 (0,0) 是 (9.5.1) 的奇点; 它 (称为) 是 (9.5.1) 的 *中心* 当且仅当

$$v_3=v_5=\cdots=v_{2j+1}=\cdots=0.$$

按这种方式给出的充分必要条件需要有限多个变元的无穷多个等式 $v_{2j+1}=0$, $j=1,2,\cdots$. 多项式 $v_3,v_5,\cdots,v_{2j+1},\cdots$ 在 $\mathrm{Q}[\boldsymbol{u}]$ 中生成的理想有有限基.

所以对任给全次数为 m 的 P 和 Q 都存在整数 N_m，使得 $v_3, v_5, \cdots, v_{2N_m+1}$ 构成这样的有限基，但问题是我们并不知道 N_m 的任何上界.

另一方面，有各种推导中心条件的方法，并且这些方法已用来求得许多具体系统中心条件的确切表达式. 遗憾的是，这些条件中有不少是错的或者是不完全的. 在下一小节中，我们将说明如何用消去法来检查中心条件的正确性以及建立不同条件之间的关系.

李雅普诺夫常数的计算和处理与微分方程定性论中的若干问题有关，并对其研究相当有用. 这些问题包括区分中心和焦点、搜索高阶焦点以及构造极限环 (后者是希尔伯特[31] 16 问题的第二部分) (参阅 [76] 和 [65] §5.4)，它们的研究形成了数学中的一个完整分支. 在处理这些问题的过程中，有时需要解多项式方程组，决定一个多项式方程是否为一组多项式方程和不等方程的推论，以及用一组多项式关系化简一个多项式等，因此消元技术在此便有用武之地. 本节中，我们并不对其进行系统地讨论，而只是就一类特殊的三次微分系统说明问题的某些方面.

库克列斯系统

以下我们介绍一个始于 1944 年的经典系统以说明消去法的应用. 笔者[74] 于 1986 年开始研究该系统；在我们的结果发表之后，数位其他学者也对同一系统进行了研究. 可是问题至今尚未解决，该系统仍然是一个挑战.

我们考虑 (9.5.1) 在

$$
\begin{aligned}
&Q(x,y) = a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3,\\
&P(x,y) = 0
\end{aligned}
\tag{9.5.2}
$$

这一特殊情形，并称该类三次微分系统为*库克列斯系统*. 库克列斯[44] 证明了此时原点为中心"当且仅当"下列四组条件之一成立:

$$
\begin{aligned}
&\alpha = a_{30}a_{11}^2 + a_{21}\lambda = 0,\\
&\beta = (3\,a_{03}\lambda + \lambda^2 + a_{12}a_{11}^2)\,a_{21} - 3\,a_{03}\lambda^2 - a_{12}a_{11}^2\lambda = 0,\\
&\gamma = \lambda + a_{20}a_{11} + a_{21} = 0,\\
&\delta = 9\,a_{12}a_{11}^2 + 2\,a_{11}^4 + 9\,\lambda^2 + 27\,a_{03}\lambda = 0;
\end{aligned}
\tag{K1}
$$

$$
a_{03} = \alpha = \beta = \gamma = 0; \tag{K2}
$$

$$
a_{03} = a_{11} = a_{21} = 0; \tag{K3}
$$

$$
a_{03} = a_{02} = a_{20} = a_{21} = 0, \tag{K4}
$$

其中 $\lambda = a_{02}a_{11} + 3\,a_{03}$. 以上条件曾被广泛认可，并被写进标准教材 (如涅梅茨基和斯捷巴诺夫的名著[60]). 库克列斯系统的近期研究则始于 20 世纪 80 年代末期，彼时金小凡与笔者[34]用格罗布讷基和特征列方法发现了下面的例子：

$$\begin{gathered} a_{20} \neq 0, \quad a_{11} = 0, \quad a_{02} = -2\,a_{20}, \quad a_{30} = -\frac{a_{20}^2}{3}, \\ a_{21}^2 = \frac{a_{20}^4}{2}, \quad a_{12} = 0, \quad a_{03} = -\frac{a_{21}}{3}; \end{gathered} \tag{JW}$$

这组条件在库克列斯的四组条件之外. 我们的计算表明，对于这一特例原点应该是中心，因此库克列斯的条件是不完全的；这一不完全性很快由克里斯托弗和劳埃德[18]确认. 之后，又有多篇论文发表，旨在给出其他特例和建立完整的中心条件. 例如，劳埃德、皮尔逊[53]和克里斯托弗一起发现了下面这组条件：

$$\begin{aligned} \kappa_1 &= 81\,a_{20}^3a_{02} - 2\,(18\,a_{11}^2r - 4\,a_{11}^4 - 27\,a_{11}^2a_{20}^2 - 81\,a_{20}^4) = 0, \\ \kappa_2 &= 9\,\eta a_{30} + 36\,a_{11}^2r + 8\,a_{11}^4 + 90\,a_{11}^2a_{20}^2 + 243\,a_{20}^4 = 0, \\ \kappa_3 &= \eta a_{21} - a_{20}a_{11}\,(27\,r - 2\,a_{11}^2 - 9\,a_{20}^2) = 0, \\ \kappa_4 &= 81\,a_{20}^2\eta a_{12} + 2\,a_{11}^2\,(144\,a_{11}^2r - 567\,a_{20}^4 - 270\,a_{11}^2a_{20}^2 \\ &\qquad + 243\,a_{20}^2r - 32\,a_{11}^4) = 0, \\ \kappa_5 &= 3\,\eta a_{03} + a_{11}\,(a_{02}\eta + 27\,a_{20}r + 14\,a_{20}a_{11}^2 + 72\,a_{20}^3) = 0, \end{aligned} \tag{CLP}$$

这里

$$\begin{aligned} \eta &= 16\,a_{11}^2 + 81\,a_{20}^2, \\ \kappa_0 &= 162\,a_{11}^2r^2 - (2\,a_{11}^2 + 9\,a_{20}^2)^3 = 0, \\ & a_{20}a_{11} \neq 0. \end{aligned}$$

另一方面，库克列斯条件的不完全性已早先由切尔卡斯[11]独立指出. 切尔卡斯用不同的方法研究了库克列斯系统，并导出了下面这组代替 (K1) 的条件：

$$\begin{aligned} \gamma &= 0, \\ \theta_1 &= 6\,a_{20}a_{03} + a_{20}a_{11}a_{02} - a_{21}a_{02} - a_{11}a_{12} - 2\,a_{30}a_{11} - \frac{2}{9}\,a_{11}^3 = 0, \\ \theta_2 &= 6\,a_{30}a_{03} - 3\,a_{20}^2a_{03} + a_{30}a_{11}a_{02} + a_{20}a_{02}a_{21} + a_{20}a_{12}a_{11} \\ &\qquad - a_{21}a_{12} - a_{30}a_{21} - \frac{2}{3}\,a_{11}^2a_{21} = 0, \\ \theta_3 &= a_{30}a_{21}a_{02} - 6\,a_{20}a_{30}a_{03} + a_{30}a_{11}a_{12} + a_{20}a_{21}a_{12} - \frac{2}{3}\,a_{11}a_{21}^2 = 0, \\ \theta_4 &= a_{30}a_{21}a_{12} - 3\,a_{30}^2a_{03} - \frac{2}{9}\,a_{21}^3 = 0; \end{aligned} \tag{C1}$$

它包含条件 (JW). 切尔卡斯并且证明了, 对 $a_{03}=0$ 他的条件与库克列斯的条件重合.

前面已经提到, 中心条件可以用不同的方法推导得出, 因此在所得条件之间可能有某种等价或者包含关系, 而未经大量计算则很难发现所有这种关系. 对库克列斯系统, 容易验证, 第三个条件 (K3) 既包含于 (K1) 又包含于 (K2), 因此是多余的. (K1) 的不可约分解由两个分支组成, 其中之一便是 (K3).

为了检查 (K1) 和 (C1) 之间的关系, 我们可以计算 (C1) 所定义的代数簇之不可约分解. 该分解的细节已在例 6.2.3 中给出.

由 (6.2.11) 以及 (K1) 的不可约分解可见, (C1) 中的两个分支与 (K1) 的两个分支重合. (C1) 的另外一个分支则给出新条件: $\mathbb{V}_2=0$. 以下我们检查这组条件与 (CLP) 之间的关系.

令 $\mathbb{P}_\kappa=\{\kappa_0,\cdots,\kappa_5\}$, 而 ω_2, $\mathbb{V}_2$ 等与例 6.2.3 中相同. 关于序 $\omega_2\prec r$, 计算 $\mathbb{P}_\kappa$ 的特征列或 $[\mathbb{P}_\kappa,\{a_{20},a_{11},\eta\}]$ 的三角序列, 我们发现

$$\mathrm{Zero}(\mathbb{P}_\kappa/a_{20}a_{11}\eta)=\mathrm{Zero}(\mathbb{T}_\kappa/a_{20}a_{11}\eta),$$

这里 $\mathbb{T}_\kappa=[\bar{T}_1,\cdots,\bar{T}_6]$; $\bar{T}_1$, $\bar{T}_2$ 和 $\bar{T}_3$ 是 $\mathbb{V}_2$ 中的第一, 第二和第四个多项式, $\bar{T}_5=\gamma$, 而

$$\begin{aligned}\bar{T}_4&=243\,a_{20}^3a_{12}+2\,(16\,a_{11}^2+27\,a_{20}^2)\,a_{11}a_{21}-4\,a_{20}\,(2\,a_{11}^2+9\,a_{20}^2)\,a_{11}^2,\\ \bar{T}_6&=-27\,a_{20}a_{11}r+3\,(2\,a_{11}^2+27\,a_{20}^2)\,a_{21}+a_{20}\,(2\,a_{11}^2+9\,a_{20}^2)\,a_{11}.\end{aligned}$$

可以验证, $\mathrm{rem}(\bar{T}_4,\mathbb{V}_2)=0$, 并且 $\mathrm{prem}(\mathbb{V}_2,\mathbb{T}_\kappa)=\{0\}$. 所以

$$\mathrm{Zero}(\mathbb{V}_2/a_{20}a_{11}\eta)=\mathrm{Zero}([\bar{T}_1,\cdots,\bar{T}_5]/a_{20}a_{11}\eta).$$

让 $\boldsymbol{a}$ 代表 $(a_{20},a_{11},a_{02},a_{30},a_{21},a_{12},a_{03})$. 于是

$$\mathrm{Zero}(\mathbb{V}_2/a_{20}a_{11}\eta)=\{\boldsymbol{a}\colon\ (\boldsymbol{a},r)\in\mathrm{Zero}(\mathbb{P}_\kappa/a_{20}a_{11}\eta)\}.$$

这就证明了条件

$$\mathbb{V}_2=0,\quad a_{20}a_{11}\eta\neq 0$$

与 (CLP) 在 $\eta\neq 0$ 时等价. 注意, 在 R 上 $\eta\neq 0$ 是 $a_{20}a_{11}\neq 0$ 的推论. 所以 (CLP) 是 (C1) 的子集, 因而是切尔卡斯条件的再发现.

$\mathbb{V}_2=0$ 在 $a_{11}=0$ 时化简为中心条件 (JW) 和

$$a_{20}=a_{11}=a_{30}=a_{21}=a_{12}=a_{03}=0,\tag{9.5.3}$$

而在 $a_{20} = 0$ 时化简为条件 (9.5.3) 和

$$a_{20} = a_{02} = a_{21} = a_{12} = a_{03} = 0, \quad 9\,a_{30} + a_{11}^2 = 0. \tag{K0}$$

(9.5.3) 包含于库克列斯条件 (K1), (K2) 和 (K3), 而 (K0) 包含于 (K4). 因此, 条件 $\mathbb{V}_2 = 0$ 已经涵盖了克里斯托弗、劳埃德、皮尔逊、金小凡和笔者所发现的库克列斯系统的全部中心条件. 综上所述, 我们有如下结果.

定理 9.5.1 中心条件 (C1) 成立当且仅当下列四组条件之一成立: (K0), (K1), (JW), (CLP).

所以, (C1), (K2) 和 (K4) 这三组条件覆盖了库克列斯系统所有已知的中心条件.

我们的符号计算方法导致了库克列斯条件不完全性的独立发现, 并用来建立了迄今所知的不同中心条件之间的不平凡关系. 对库克列斯系统的公式推导表明, 这方面的工作紧密依赖于消去法的系统运用.

有了切尔卡斯条件 (C1) 并不妨碍我们进一步研究库克列斯系统. 这是因为切尔卡斯所用的方法亦有疑点. 笔者发现, 他对其他微分系统所导出的某些条件也不完全. 这一不完全性后来由劳埃德和皮尔逊确认.

中心条件的推导

推导中心的必要条件可以部分地化为分解大多项式系统, 对此所用的主要计算工具是基于特征列、格罗布纳基和结式的消元技术. 实践表明, 中心条件的推导是一个相当棘手、难于驾驭的问题, 原因是所遇到的多项式次数太高、项数太多而无法对付.

为了计算, 我们选取适当的 N, 构造多项式组

$$\mathbb{P}_N = \{v_3, v_5, \cdots, v_{2N+1}\},$$

并简化或求解 $\mathbb{P}_N = 0$ 以便得到原点为中心的必要条件. 条件的充分性 —— 即 $\mathbb{P}_N = 0$ 蕴涵着 $v_{2j+1} = 0$ 对所有 $j > N$ 成立 —— 则需用复杂的数学技巧另加证明.

我们先后用 Fortran, Scratchpad II 和 Maple 编制了计算任意中心焦点型微分系统李雅普诺夫常数的程序, 称为 DEMS. 对库克列斯系统, 第一个李雅普诺夫常数为 $v_3 = \gamma/3$. 为了简化计算, 我们用

$$-(3\,a_{03} + a_{11}a_{02} + a_{11}a_{20})$$

替换 (9.5.2) 中的 a_{21}, 那么 $v_3 = 0$, 而经 DEMS 计算得出的后面 8 个李雅普诺夫常数具有如下特征：

	v_5	v_7	v_9	v_{11}	v_{13}	v_{15}	v_{17}	v_{19}
项数	13	49	131	292	577	1046	1775	2859
全次数	4	6	8	10	12	14	16	18
系数位数	2	4	6	9	13	17	22	27

表中“系数位数”是指整系数的最大位数. 读者可以通过互联网从 `http://calfor.lip6.fr/~wang/PEAA/Wang.html` 下载这些 (Maple 格式的) 多项式. 库克列斯问题部分地化为化简 $\mathbb{P}_N = 0$ 给出的条件以及检查它们与已知中心条件之间的关系.

(C1), (K2) 和 (K4) 是否涵盖库克列斯系统的所有中心条件这一问题似乎仍无定论. 按照文献 [53] 中的定理 4.1 和前节中的结果, 库克列斯系统不再有 (C1), (K2) 和 (K4) 以外的高维中心条件. 事实上, 劳埃德和皮尔逊猜测库克列斯系统根本就不再有其他中心条件. 搜索中心条件的困难主要是由所牵涉的大规模多项式计算引起的. 尽管如此, 当我们去处理那些庞大、看上去奇特而又像有规则可循的多项式时, 我们经常又能看到获得新中心条件的一线希望而备受鼓舞.

从库克列斯系统的已知中心条件可见, 对较大的 N 代数簇 Zero($\mathbb{P}_N$) 应该是可约的. 因此自然的想法是将 $\mathbb{P}_N$ 分解为不可约分支. 可是由于 $\mathbb{P}_N$ 中的多项式太大, 将前面提到的消去算法简单地用于 $\mathbb{P}_N$ 则不会成功. 随着 N 的增大, 可约性会出现, 因而将 $\mathbb{P}_N$ 分裂为子系统成为可能. 在分裂之后, 我们得到较小的子系统, 因此所牵涉的计算将会变得相对容易. 不幸的是, 多项式 v_{2N+1} 随着 N 的增大而迅速扩大. 所以太大的 N 也同样会引起麻烦.

我们选取 $N = 7$, 并作了多种尝试包括交互式消元以将多项式组 $\mathbb{P}_7$ 分解为不可约三角系统而未能成功. 分解 $\mathbb{P}_7$ 以及对库克列斯系统建立完整的中心条件仍然是尚未解决的挑战性问题.

文献注记

虽然在使用他人的工作和材料时我们尽量注明其出处，但在某些情形我们可能忘记或者没有恰当地将所引用的结果归功于原作者. 对此和其他任何不适当的疏忽，我们在此表示歉意. 这里对有关历史和文献作若干附加注记，其中有些因与上下文不太衔接而未在相应章节中给出，而其他附注的有意重复则是为了强调.

小　议

在西方，消去理论从 18 世纪开始发展起来. 早期的方法源于欧拉 [23] 和贝佐 [4], 而最著名的则是解线性方程组的高斯消去法 [27] 和解一般多项式方程组的西尔维斯特析配法 [67]. 前者极为基本，有非常广泛的应用，而后者始自对代数不变量的研究，并经大英学派的凯莱、狄克逊和麦考莱等人逐步发展为结式理论.

以高斯命名的将线性方程组三角化的方法早已见之于中国的经典巨著《*九章算术*》(以下简称《*九章*》), 该书公元前后成型，并由刘徽于公元 260 年前后作注.《九章》一书的体系是先提出日常生活中的问题，然后给出其解答以及求得这一解答的方法. 解下列 (三个) 线性方程组的例子源自第八章 (*方程术*), 它是该书中 246 个问题之一:

$$\begin{cases} 3x + 2y + z = 39, \\ 2x + 3y + z = 34, \\ x + 2y + 3z = 26. \end{cases}$$

《九章》中给出的方法先将这些方程的系数和常数项排列成矩阵形式，然后通过列之间的运算将该矩阵化为三角矩阵. 后者表示方程 $36z = 99$, $5y+z = 24$ 和 $3x + 2y + z = 39$, 由此容易依次求得 z, y 和 x 的值. 有关细节，读者可参阅《九章》原著，刘徽的《注九章算术》以及 [5] (第 218 和 219 页), [59] (24—28, 115 和 116 页) 与 [73] (47 至 49 页).

用 18 个问题加以说明的 *方程术* 能处理任意多个未知数的联立线性方程组，并且使用了负数. 最后一个问题涉及四个方程和五个未知数，因而导致不定方程.《九章》中描述的方法既系统又有效，它与高斯在 1826 年提出的消

去法具有同样的算法特征，可谓异曲同工．鉴于这一事实而《九章》的著者已难于考证，吴文俊称上述方法为 *中国－高斯消去法*．事实上，该方法在数学史籍中已被称为 *中国矩阵法* (见 [5] 第 248 页)．本书中所描述的若干算法都可视为中国－高斯消去法的推广．

最广为人知、解联立高次代数方程组和判定这类方程组之可解性的消去法则是基于结式．另一方面，对一般消去法的探索在中国由来已久．迄 13 世纪宋元时期，中国代数学家就已创立了一套方法，称之为 *四元术*，它可以用来求解四个未知数以内的任意高次多项式方程组．多项式运算与消元是中国古代数学成就中的重要典范．那时所发展起来的方法不仅用于求解代数方程而且也作为代数工具用来系统地处理几何问题．

作为以上议论的结尾，我们将祖颐季为朱世杰 (1303 年) 的《四元玉鉴》所作序言中的一段道家玄论摘录如下．

> “上升下降左右进退互通变化乘除往来用假象真以虚问实错综正负分成四式必以寄之剔之餘筹易位横冲直撞精而不杂自然而然消而和会以成开方之式也”

第一章

本章中的材料出处不尽相同，但读者能从 [71, 72] 和 [41] 中查到大部分概念和结果．子结式的介绍则基于 [57] 中的第七章．

第二至第四章

特征列的概念和方法是里特[61, 62]对微分多项式理想引进的．吴文俊在 20 世纪 70 年代后期首先认识到了里特方法的效力，并对多项式组 (而不是理想) 大大改进和发展了这一方法．特别值得一提的是，吴去掉了不可约性条件使定义并在不同意义下计算任意多项式组的特征列成为可能．吴文俊[95, 96, 97, 100, 101]及其领导的数学机械化研究组的成员[58]、周咸青[16]、高小山[26]、加罗和米施拉[24]以及笔者本人[79, 83]等都为特征列方法的改进和发展做了大量工作．本书中特征列方法的论述则基于笔者的讲稿[75]和吴的著作[96]．

2.3 和 4.2 节中所描述的消去算法源于赛登贝格[63, 64]的消去理论．笔者[81]对其作了适当的改进．正则列的概念是卡尔克布伦讷[35]和杨路、张景中[105]独立引进的；前者称其为 *正则链*，而后者则称其为 *正常升链*．高小山和周咸青[26]也做了与之有关的工作．

简单系统的概念出自托马斯[68]的经典著作. 2.4, 3.1 和 3.3 节中使用子结式正则子链的分解算法均由笔者[88, 90]提出, 对此我们受益于米施拉[57]关于子结式的论述. 若干有关正则和简单系统的性质也是笔者首先证明的.

4.3 至 4.5 节中的内容大多取自 [95, 97, 96] 和 [81].

第五章

5.2 节的写作受到了拉扎尔[49]工作的激励.

格罗布讷基方法是布赫贝格尔[7]的重要发现. 5.3 节中的大部分材料源自 [8]. 格罗布讷基的历史以及丰富的文献见诸于 [1, 3]. 5.4 节的基础是 [71] 中的第十一章和 [39, 12], 这些著作提供了大量历史与文献资料.

第六章

维数和非混合分解的部分论述基于周咸青[16]、高小山[26]和卡尔克布伦讷[35]的工作, 但这里稍有推广. 里特[62]、吴文俊[102]、周咸青等[17]和笔者[75]都分别提出了计算不可约升列素基的方法. 使用格罗布讷基构造浸润基的技巧也见之于吉安尼等人的论著[28]. 笔者在 [75, 78] 中研究了代数簇的不可约分解. 准素理想分解的算法归功于下山武司和横山和弘[66].

第八、第九章

众多学者对几何学定理机器证明的研究和发展作出了贡献; 在综述 [87] 中和网页 `http://calfor.lip6.fr/~wang/GRBib` 上, 读者可以看到很长的文献目录. 我们应该特别提到吴文俊[94, 95, 99, 96]及其学生[92, 58]、周咸青[14]、卡普尔[38]、库茨勒和施蒂夫特[47]等人的工作. 周在 [14] 中给出了使用吴方法和格罗布讷基方法证明的 512 个几何定理. 高海萍[42]、周和高小山[16]以及笔者[85]还将零点分解用于几何定理机器证明.

未知关系的自动发现或推导由吴文俊[98]和周咸青[13]发起; 周后来与高小山合作[15]加之笔者[84]又对其作了进一步的研究. 多位学者研究了参数对象的隐式化; 有关背景和文献信息, 读者可参阅 [9, 51]. 9.4 节中描述的代数因子分解方法分别取自 [32] 和 [80]. 消去法的若干其他几何应用见诸于 [9, 84, 58].

参 考 文 献

[1] Adams, W. W., Loustaunau, P.: An introduction to Gröbner bases. American Mathematical Society, Providence (1994).

[2] Aubry, P., Lazard, D., Moreno Maza, M.: On the theories of triangular sets. J. Symb. Comput. **28** (1999): 105–124.

[3] Becker, T., Weispfenning, V.: Gröbner bases: A computational approach to commutative algebra. Springer, New York Berlin Heidelberg (1993).

[4] Bézout, É.: Théorie générale des équations algébriques. Ph.D. thesis, Pierres, Paris (1779).

[5] Boyer, C. B.: A history of mathematics. John Wiley & Sons, New York London Sydney (1968).

[6] Brown, W. S., Traub, J. F.: On Euclid's algorithm and the theory of subresultants. J. ACM **18** (1971): 505–514.

[7] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. thesis, Universität Innsbruck, Austria (1965).

[8] Buchberger, B.: Gröbner bases: An algorithmic method in polynomial ideal theory. In: Bose, N. K. (ed.): Multidimensional systems theory. Reidel, Dordrecht, pp. 184–232 (1985).

[9] Buchberger, B.: Applications of Gröbner bases in non-linear computational geometry. In: Rice, J. R. (ed.): Mathematical aspects of scientific software. Springer, New York Berlin Heidelberg, pp. 59–87 (1987).

[10] Buchberger, B., Collins, G. E., Kutzler, B.: Algebraic methods for geometric reasoning. Ann. Rev. Comput. Sci. **3** (1988): 85–119.

[11] Cherkas, L. A.: Conditions for the equation $yy' = \sum_{i=0}^{3} p_i(x)y^i$ to have a center. Differentsial'nye Uravneniya **14** (1978): 1594–1600.

[12] Chionh, E. W., Goldman, R. N.: Elimination and resultants. IEEE Comput. Graphics Appl. **15**/1 (1995): 69–77; **15**/2 (1995): 60–69.

[13] Chou, S.-C.: A method for the mechanical derivation of formulas in elementary geometry. J. Automat. Reason. **3** (1987): 291–299.

[14] Chou, S.-C.: Mechanical geometry theorem proving. Reidel, Dordrecht (1988).

[15] Chou, S.-C., Gao, X.-S.: Mechanical formula derivation in elementary geometries. In: Proceedings ISSAC '90, Tokyo, August 20–24, 1990. ACM Press, New York, pp. 265–270.

[16] Chou, S.-C., Gao, X.-S.: Ritt–Wu's decomposition algorithm and geometry theorem proving. In: Proceedings CADE-10, Kaiserslautern, July 24–27, 1990. Springer, Berlin Heidelberg New York Tokyo, pp. 207–220 (Lecture notes in computer science, vol. 449) [also as Tech. Rep. TR-89-09, Department of Computer Science, The University of Texas at Austin, USA].

[17] Chou, S.-C., Schelter, W. F., Yang, J.-G.: An algorithm for constructing Gröbner bases from characteristic sets and its application to geometry. Algorithmica **5** (1990): 147–154.

[18] Christopher, C. J., Lloyd, N. G.: On the paper of Jin and Wang concerning the conditions for a centre in certain cubic systems. Bull. London Math. Soc. **22** (1990): 5–12.

[19] Collins, G. E.: Subresultants and reduced polynomial remainder sequences. J. ACM **14** (1967): 128–142.

[20] Collins, G. E.: The calculation of multivariate polynomial resultants. J. ACM **18** (1971): 515–532.

[21] Cox, D., Little, J., O'Shea, D.: Ideals, varieties, and algorithms. Springer, New York Berlin Heidelberg (1992).

[22] Dixon, A. L.: The eliminant of three quantics in two independent variables. Proc. London Math. Soc. **6** (1908): 468–478.

[23] Euler, L.: Elements of algebra. Longman, Orme, and Co., London (1840) [translated by J. Hewlett; reprinted by Springer (1984)].

[24] Gallo, G., Mishra, B.: Efficient algorithms and bounds for Wu–Ritt characteristic sets. In: Proceedings MEGA '90, Livorno, April 17–21, 1990. Birkhäuser, Boston, pp. 119–142 (1991) (Progress in mathematics, vol. 94).

[25] Gao, X.-S., Chou, S.-C.: Solving parametric algebraic systems. In: Proceedings ISSAC '92, Berkeley, July 27–29, 1992. ACM Press, New York, pp. 335–341 [also in Math. Mech. Res. Preprints 7 (1992): 14–30].

[26] Gao, X.-S., Chou, S.-C.: On the dimension of an arbitrary ascending chain. Chinese Sci. Bull. **38** (1993): 799–804.

[27] Gauss, C. F.: Werke. Band IV, Herausgegeben von der Königlichen Gesellschaft der Wissenshaft zu Göttingen (1873).

[28] Gianni, P., Trager, B. M., Zacharias, G.: Gröbner bases and primary decomposition of polynomial ideals. J. Symb. Comput. **6** (1988): 149–167.

[29] Hartshorne, R.: Algebraic geometry. Springer, Berlin New York (1977).

[30] 何青：计算代数. 北京师范大学出版社，北京 (1997).

[31] Hilbert, D.: Mathematische Probleme. Arch. Math. Phys. (3) **1** (1901): 44–63; 213–237.

[32] 胡森、王东明：有理数域及其代数扩域上的快速因子分解. 科学通报，1985 年第 20 期：1525–1529.

[33] Jacobson, N.: Basic algebra I. Freeman, San Francisco (1974).

[34] Jin, X., Wang, D.: On the conditions of Kukles for the existence of a centre. Bull. London Math. Soc. **22** (1990): 1–4.

[35] Kalkbrener, M.: A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. J. Symb. Comput. **15** (1993): 143–167.

[36] Kalkbrener, M.: Prime decompositions of radicals in polynomial rings. J. Symb. Comput. **18** (1994): 365–372.

[37] Kapur, D.: Using Gröbner bases to reason about geometry problems. J. Symb. Comput. **2** (1986): 399–408.

[38] Kapur, D.: A refutational approach to geometry theorem proving. Artif. Intell. **37** (1988): 61–93.

[39] Kapur, D., Lakshman, Y. N.: Elimination methods: An introduction. In: Donald, B. R., Kapur, D., Mundy, J. L. (eds.): Symbolic and numerical computation for artificial intelligence. Academic Press, London New York Sydney, pp. 45–87 (1992).

[40] Kapur, D., Saxena, T.: Comparison of various multivariate resultant formulations. In: Proceedings ISSAC '95, Montreal, July 10–12, 1995. ACM Press, New York, pp. 187–194.

[41] Knuth, D. E.: The art of computer programming, vol. 2. 2nd ed. Addison-Wesley, Reading London Amsterdam (1981).

[42] Ko, H.-P.: Geometry theorem proving by decomposition of quasi-algebraic sets: An application of the Ritt–Wu principle. Artif. Intell. **37** (1988): 95–122.

[43] Ko, H.-P., Hussain, M. A.: ALGE-prover: An algebraic geometry theorem proving software. Tech. Rep. 85CRD139, General Electric Company, Schenectady, USA (1985).

[44] Куклес, И. С.: О необходимых и достаточных условиях наличия центра, ДАН **42** (1944): 160–163.

[45] Kusche, K., Kutzler, B., Stifter, S.: Implementation of a geometry theorem proving package in Scratchpad II. In: Proceedings EUROCAL '87, Leipzig, June 2–5, 1987. Springer, Berlin Heidelberg, pp. 246–257 (1989) (Lecture notes in computer science, vol. 387).

[46] Kutzler, B.: Algebraic approaches to automated geometry theorem proving. Ph.D. thesis, Johannes Kepler University, Linz, Austria (1988).

[47] Kutzler, B., Stifter, S.: On the application of Buchberger's algorithm to automated geometry theorem proving. J. Symb. Comput. **2** (1986): 389–397.

[48] Lazard, D.: Résolution des systèmes d'équations algébriques. Theor. Comput. Sci. **15** (1981): 77–110.

[49] Lazard, D.: A new method for solving algebraic systems of positive dimension. Discrete Appl. Math. **33** (1991): 147–160.

[50] Li, Z.-M.: Determinant polynomial sequences. Chinese Sci. Bull. **34** (1989): 1595–1599.

[51] Li, Z.-M.: Automatic implicitization of parametric objects. Math. Mech. Res. Preprints 4 (1989): 54–62.

[52] Liu, Z.-J.: An algorithm for finding all isolated zeros of polynomial systems. In: Proceedings ISSAC '90, Tokyo, August 20–24, 1990. ACM Press, New York, p. 300.

[53] Lloyd, N. G., Pearson, J. M.: Computing centre conditions for certain cubic systems. J. Comput. Appl. Math. **40** (1992): 323–336.

[54] Loos, R.: Generalized polynomial remainder sequences. In: Buchberger, B., Collins, G. E., Loos, R. (eds.): Computer algebra: Symbolic and algebraic computation, 2nd ed. Springer, Wien New York, pp. 115–137 (1983).

[55] Macaulay, F. S.: Note on the resultant of a number of polynomials of the same degree. Proc. London Math. Soc. **21** (1921): 14–21.

[56] Macaulay, F. S.: The algebraic theory of modular systems. Stechert-Hafner Service Agency, New York London (1964) [originally published in 1916 by Cambridge University Press, Cambridge].

[57] Mishra, B.: Algorithmic algebra. Springer, New York (1993).

[58] 中国科学院系统科学研究所数学机械化研究中心编印：数学机械化与机械化数学研究报告. 1987 年第 1 期至 1996 年第 14 期.

[59] Needham, J.: Science and civilisation in China, vol. 3. Cambridge University Press, Cambridge (1959).

[60] 涅梅茨基, B. B., 斯捷巴诺夫, B. B.: 微分方程定性论 (上册). 科学出版社, 北京 (1956) [王柔怀、童勤谟译自俄文].

[61] Ritt, J. F.: Differential equations from the algebraic standpoint. American Mathematical Society, New York (1932).

[62] Ritt, J. F.: Differential algebra. American Mathematical Society, New York (1950).

[63] Seidenberg, A.: Some remarks on Hilbert's Nullstellensatz. Arch. Math. **7** (1956): 235–240.

[64] Seidenberg, A.: An elimination theory for differential algebra. Univ. California Publ. Math. (N.S.) **3**/2 (1956): 31–66.

[65] 石赫：机械化数学引论. 湖南教育出版社，长沙 (1998).

[66] Shimoyama, T., Yokoyama, K.: Localization and primary decomposition of polynomial ideals. J. Symb. Comput. **22** (1996): 247–277.

[67] Sylvester, J. J.: The collected mathematical papers, vol. I. Cambridge University Press, Cambridge (1904).

[68] Thomas, J. M.: Differential systems. American Mathematical Society, New York (1937).

[69] Thomas, J. M.: Division sequence. Duke Math. J. **13** (1946): 459–469.

[70] Trager, B. M.: Algebraic factoring and rational function integration. In: Proceedings SYMSAC '76, Yorktown Heights, August 10–12, 1976. ACM Press, New York, pp. 219–226.

[71] van der Waerden, B. L.: Modern algebra, vol. II. Frederick Ungar, New York (1950) [translated from the German edition — published in 1931, 1937 and 1940 by Springer, Berlin — by T. J. Benac].

[72] van der Waerden, B. L.: Modern algebra, vol. I. Frederick Ungar, New York (1953) [translated from the second revised German edition — published in 1937 and 1940 by Springer, Berlin — by F. Blum].

[73] van der Waerden, B. L.: Geometry and algebra in ancient civilizations. Springer, Berlin Heidelberg New York Tokyo (1983).

[74] 王东明：多项式组及其相关问题的机械化研究. 中国科学院博士论文，北京 (1987).

[75] Wang, D.: Characteristic sets and zero structure of polynomial sets. Lecture Notes, RISC-Linz, Johannes Kepler University, Austria (1989–1995) [also available from http://calfor.lip6.fr/~wang/manu.html].

[76] Wang, D.: Mechanical manipulation for a class of differential systems. J. Symb. Comput. **12** (1991): 233–254.

[77] Wang, D.: On the parallelization of characteristic-set-based algorithms. In: Proceedings 1st Int. ACPC Conf., Salzburg, September 30 – October 2, 1991. Springer, Berlin Heidelberg New York Tokyo, pp. 338–349 (Lecture notes in computer science, vol. 591).

[78] Wang, D.: Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases. Comput. Aided Geom. Design **9** (1992): 471–484.

[79] Wang, D.: A strategy for speeding-up the computation of characteristic sets. In: Proceedings MFCS '92, Prague, August 24–28, 1992. Springer, Berlin Heidelberg New York Tokyo, pp. 504–510 (Lecture notes in computer science, vol. 629).

[80] Wang, D.: A method for factorizing multivariate polynomials over successive algebraic extension fields. Preprint. RISC-Linz, Johannes Kepler University, Austria (1992) [also available from http://calfor.lip6.fr/~wang/ manu.html].

[81] Wang, D.: An elimination method for polynomial systems. J. Symb. Comput. **16** (1993): 83–114.

[82] Wang, D.: Algebraic factoring and geometry theorem proving. In: Proceedings CADE-12, Nancy, June 28 – July 1, 1994. Springer, Berlin Heidelberg New York Tokyo, pp. 386–400 (Lecture notes in artificial intelligence, vol. 814).

[83] Wang, D.: An implementation of the characteristic set method in Maple. In: Pfalzgraf, J., Wang, D. (eds.): Automated practical reasoning: Algebraic approaches. Springer, Wien New York, pp. 187–201 (1995).

[84] Wang, D.: Reasoning about geometric problems using an elimination method. In: Pfalzgraf, J., Wang, D. (eds.): Automated practical reasoning: Algebraic approaches. Springer, Wien New York, pp. 147–185 (1995).

[85] Wang, D.: Elimination procedures for mechanical theorem proving in geometry. Ann. Math. Artif. Intell. **13** (1995): 1–24.

[86] Wang, D.: GEOTHER: A geometry theorem prover. In: Proceedings CADE-13, New Brunswick, July 30 – August 3, 1996. Springer, Berlin Heidelberg New York Tokyo, pp. 166–170 (Lecture notes in artificial intelligence, vol. 1104).

[87] Wang, D.: Geometry machines: From AI to SMC. In: Proceedings AISMC-3, Steyr, September 23–25, 1996. Springer, Berlin Heidelberg New York Tokyo, pp. 213–239 (Lecture notes in computer science, vol. 1138).

[88] Wang, D.: Decomposing polynomial systems into simple systems. J. Symb. Comput. **25** (1998): 295–314.

[89] Wang, D.: Elimination methods and applications. Habilitation thesis, Institut National Polytechnique de Grenoble, France (1999).

[90] Wang, D.: Computing triangular systems and regular systems. J. Symb. Comput. **30** (2000): 221–236.

[91] Wang, D.: Elimination methods. Springer, Wien New York (2001).

[92] Wang, D., Gao, X.-S.: Geometry theorems proved mechanically using Wu's method — Part on Euclidean geometry. Math. Mech. Res. Preprints 2 (1987): 75–106.

[93] Winkler, F.: Gröbner bases in geometry theorem proving and simplest degeneracy conditions. Math. Pannonica **1** (1990): 15–32.

[94] 吴文俊：初等几何判定问题与机械化证明．中国科学，1977 年第 6 期：507–516.

[95] Wu, W.-t.: Basic principles of mechanical theorem proving in elementary geometries. J. Syst. Sci. Math. Sci. **4** (1984): 207–235 [also in J. Automat. Reason. **2** (1986): 221–252].

[96] 吴文俊：几何定理机器证明的基本原理 (初等几何部分). 科学出版社，北京 (1984). 英译本 (1994): Mechanical theorem proving in geometries: Basic principles. Springer, Wien New York [金小凡、王东明译].

[97] 吴文俊：关于代数方程组的零点 —— Ritt 原理的一个应用. 科学通报，1985 年第 12 期：881–883.

[98] Wu, W.-t.: A mechanization method of geometry and its applications I. Distances, areas and volumes. J. Syst. Sci. Math. Sci. **6** (1986): 204–216.

[99] Wu, W.-t.: On reducibility problem in mechanical theorem proving of elementary geometries. Chinese Quart. J. Math. **2** (1986): 1–20.

[100] Wu, W.-t.: A zero structure theorem for polynomial equations-solving. Math. Mech. Res. Preprints 1 (1987): 2–12.

[101] Wu, W.-t.: Some remarks on characteristic-set formation. Math. Mech. Res. Preprints 3 (1989): 27–29.

[102] Wu, W.-t.: On the generic zero and Chow basis of an irreducible ascending set. Math. Mech. Res. Preprints 4 (1989): 1–21.

[103] Wu, W.-t.: On a projection theorem of quasi-varieties in elimination theory. Chinese Ann. Math. (Ser. B) **11** (1990): 220–226.

[104] 吴文俊、吕学礼：分角线相等的三角形. 人民教育出版社，北京 (1985).

[105] Yang, L., Zhang, J.-Z.: Searching dependency between algebraic equations: An algorithm applied to automated reasoning. In: Johnson, J., McKee, S., Vella, A. (eds.): Artificial intelligence in mathematics. Oxford University Press, Oxford, pp. 147–156 (1994).

[106] Yang, L., Zhang, J.-Z., Hou, X.-R.: An efficient decomposition algorithm for geometry theorem proving without factorization. In: Proceedings ASCM '95, Beijing, August 18–20, 1995. Scientists Inc., Tokyo, pp. 33–41.

[107] 杨路、张景中、侯晓荣：非线性代数方程组与定理机器证明. 上海科技教育出版社，上海 (1996).

索 引

(汉 英 对 照)

一至三画

四 画

五 画

六 画

七 画

八 画

九 画

十 画

十一画

十二画

十三画

十四画

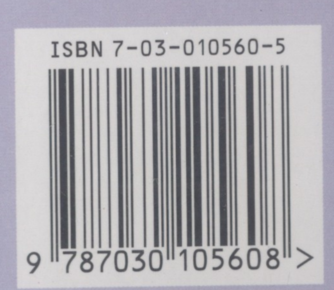
十五画以上

其 他

(O-1638.1101)
● 责任编辑：吕　虹
● 封面设计：黄华斌

数学机械化丛书(部分书目)

- 数学机械化—方程与几何问题求解　吴文俊
- 几何定理机器证明的几何不变量方法　张景中、高小山、周咸青
- 消去法及其应用　王东明
- 组合恒等式的机器证明　陈永川
- 几何自动作图与智能CAD　高小山
- 代数曲面造型　陈发来 等
- 非线性数学物理方程的行波解　李志斌 等



ISBN 7-03-010560-5/O・1638
定　价：48.00元